View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Electronic Thesis and Dissertation Archive - Università di Pisa

Università Degli Studi di Pisa
Facoltà di Scienze Matematiche, Fisiche e Naturali
Corso di Laurea in Matematica

Tesi di Laurea Specialistica

Salti della ramificazione nelle p-estensioni cicliche dei campi p-adici.

Candidato
Laura Capuano

Relatore
Prof.ssa Ilaria Del Corso

Controrelatore
Prof. Roberto Dvornicich

Anno Accademico 2009/2010

Introduzione

Il proposito della tesi è quello di studiare le proprietà principali della filtrazione dei gruppi di ramificazione con indice in alto nelle estensioni di Galois finite di campi locali, dandone una completa caratterizzazione nel caso di estensioni cicliche totelmente ramificate di grado p^m.

Fissiamo un campo K completo rispetto ad una valutazione discreta v_K con campo dei residui di caratteristica $p > 0$; detta L una sua estensione finita allora v_K ammette un'unica estensione ad L che chiamiamo v_L. Indichiamo con $\mathcal{O}_L$ l'anello di valutazione di L rispetto a v_L.

Supponiamo in aggiunta che L/K sia di Galois con gruppo di Galois G: $\forall i \geq -1$ reale si definisce l'i-esimo gruppo di ramificazione di L/K come

$$G_i = \{\sigma \in G \mid v_L(\sigma(a) - a) \geq i + 1 \ \forall \ a \in \mathcal{O}_L\}.$$

La successione dei G_i costituisce una filtrazione del gruppo di Galois G dell'estensione tale che $\forall i \geq -1$ $G_{i+1} \lhd G_i$ e definitivamente $G_n = \{e\}$.
Definiamo inoltre la funzione

$$\varphi_{L/K}(s) = \int_0^s \frac{dx}{|G_0 : G_x|} \, .$$

Detta allora $\psi_{L/K}$ l'inversa di $\varphi_{L/K}$ definiamo i gruppi di ramificazione con indice in alto come $G^t =: G_{\psi_{L/K}(t)}$. Un numero reale t è detto salto della ramificazione in alto se $G^t \neq G^u \ \forall u > t$.
Il teorema di Hasse-Arf [Arf] afferma che, nel caso di estensioni abeliane, i salti della ramificazione in alto sono interi.

Un problema classico è trovare condizioni necessarie e sufficienti affiché, data una m-pla di interi $\{t^1, \ldots, t^m\}$, esista un'estensione ciclica totalmente ramificata K_m/K di grado p^m tale che i salti in alto dei gruppi di ramificazione siano esattamente $\{t^1, \ldots, t^m\}$.

La soluzione del problema risulta direttamente legata alla presenza di radici p^s-esime dell'unità nel campo K di partenza.
Una prima soluzione infatti è stata data dal matematico tedesco E. Maus

[Mau1] in due casi particolari: il primo, in cui K non contiene radici p-esime dell'unità, e il secondo in cui K contiene una radice p-esima dell'unità e $v_K(\zeta_p - 1)$ non è divisibile per p. Successivamente, analizzando il caso in cui $\zeta_p \in K$, il matematico americano B.Wiman [Wym] ha dimostrato la condizione necessaria

$$t^{i+1} = t^i + e \quad \forall i \geq c,$$

dove c è una costante che dispende soltanto dal campo K ed $e = v_K(p)$, usando soltanto la teoria di Kummer. Nello stesso periodo ma utilizzando strumenti più sofisticati, il matemitico canadese M.Marshall [Mar] ha dimostrato che, detto $e' = e/(p-1)$, le condizioni:

(a) $1 \leq t^1 \leq pe'$ e $(t^1, p) = 1$ se $t^1 \neq pe'$;

(b) se $t^i < e'$ allora $pt^i \leq t^{i+1} \leq pe'$ e $(t^{i+1}, p) = 1$ se $t^{i+1} \neq pt^i, pe'$;

(c) se $t^i \geq e'$ allora $t^{i+1} = t^i + e$

sono necessarie, mostrandone anche la sufficienza nel caso in cui $t^{m-1} < e'$. In seguito, il matematico francese T.Nguyen-quang-do [Ngu] ha fornito una dimostrazione più diretta dell'ultima proprietà nel caso in cui K contenga le radici p-esime dell'unità.

La soluzione definitiva del problema nel caso in cui $|\overline{K}| < +\infty$ è stata data dal matematico giapponese H. Miki [Mik1]. La trattazione di Miki evidenzia che, nel caso in cui $\zeta_p \in K$ e $v_K(\zeta_p - 1) \equiv 0 \ (p)$, l'esistenza di una certa relazione tra alcuni generatori del gruppo U_K^1 come $\mathbb{Z}_p$ -modulo rende molto più difficile determinare i possibili salti della ramificazione, ma la dimostrazione non è costruttiva.

Nonostante la semplicità dell'enunciato del problema, la trattazione nel caso generale richiede l'utilizzo di strumenti abbastanza sofisticati di teoria algebrica dei numeri quali la class field e lo studio del comportamento della norma ristretta al gruppo delle unità U_L; a tali arogmenti è infatti dedicata la prima parte della tesi.
Nell'ipotesi in cui il campo dei residui di K sia finito, il teorema di esistenza della class field [FeV] asserisce che esiste una corrispondenza biunivoca tra i sottogruppi N di K^* di indice finito e le estensioni abeliane finite L di K tale che $N = N_{L/K}(L^*)$. Inoltre, da tale corrispondenza discende anche un isomorfismo tra il gruppo di Galois G dell'estensione e il gruppo finito $K^*/N_{L/K}(L^*)$. Tale teorema permette quindi di trasformare la ricerca di estensioni cicliche di grado p^m nello studio di sottogruppi N di K^* tali che il gruppo quoziente K^*/N sia ciclico di ordine p^m. Inoltre, tramite lo studio delle proprietà delle norme, si dimostra che data un'estensione L/K ciclica di grado p^m e detto N

il sottogruppo delle norme associato all'estensione, l'i-esimo salto in alto della ramificazione t^i è il minimo intero j tale che $U_K^{j+1} \subset NK^{*p^i}$. Tale proprietà permette quindi di imporre le condizioni affinché, preso un sottogruppo N di K^* con le proprietà descritte precedentemente l'estensione ad esso associata abbia i salti della ramificazione cercati.

La seconda parte dell'elaborato dà una dimostrazione completa dei principali risultati sia di Maus che di Miki. In particolare, la sufficienza delle condizioni è dimostrata in modo diretto fornendo, in ognuno dei casi possibili, una costruzione esplicita del sottogruppo normico $N \subset K^*$ associato all'estensione cercata (tramite la class field) usando le proprietà di una particolare base del gruppo delle unità.

La tesi contiene infine anche alcuni esempi concreti dell'applicazione del teorema di Miki. Il caso delle estensioni cicliche di grado p può essere trattato in modo diretto senza l'aiuto della class field. Infatti, se il campo K contiene le radici p-esime dell'unità allora ogni estensione di grado p su K è della forma $K(\sqrt[p]{a})$ con $a \in K$; in questo caso quindi utilizzando il calcolo esplicito del differente dell'estensione è possibile determinare il salto dell'estensione in funzione della valutazione di a. Da tale caso discende anche una trattazione delle proprietà dei salti di estensioni totalmente ramificate con gruppo di Galois $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Un altro esempio largamente approfondito è il caso delle estensioni ciclotomiche di $\mathbb{Q}_p$. Se consideriamo come campo di partenza $K = \mathbb{Q}_p(\zeta_{p^s})$, allora $v_K(\zeta_{p^s} - 1) = 1 \not\equiv 0 \ (p)$; anche in questo caso quindi le condizioni possono essere descritte in modo più diretto.

Indice

Capitolo 1

Richiami preliminari

1.1 Campi completi: proprietà generali

Sia K un campo completo rispetto ad una valutazione discreta v_K. Indichiamo con $\mathcal{O}_K$ il rispettivo anello di valutazione e con $\mathcal{M}_K$ il suo unico ideale massimale; siano inoltre $\overline{K} = \mathcal{O}_K/\mathcal{M}_K$ il campo dei residui di K e $U_K = \mathcal{O}_K - \mathcal{M}_K$ il gruppo moltiplicativo degli elementi invertibili di $\mathcal{O}_K$.
Fissiamo un generatore π dell'ideale $\mathcal{M}_K$; tale elemento è detto uniformizzante di K.

Definizione 1.1. Un insieme R è detto insieme di rappresentanti per un campo K se $R \subset \mathcal{O}_K$, $0 \in R$ e la restrizione ad R della mappa canonica $\mathcal{O}_K \longrightarrow \mathcal{O}_K/\mathcal{M}_K = \overline{K}$ è bigettiva. Denotiamo con $rep : \overline{K} \to R$ l'inversa dell'applicazione precedente. Per un insieme S denotiamo con $(S)_n^{+\infty}$ l'insieme delle successioni $(a_i)_{i\geq n}$ e $a_i \in S$ e con $(S)_{-\infty}^{+\infty}$ l'unione crescente degli insiemi $(S)_n^{+\infty}$ dove $n \to -\infty$.

Notiamo che il gruppo additivo K ha una filtrazione naturale

$$\ldots \supset \pi^i\mathcal{O}_K \supset \pi^{i+1}\mathcal{O}_K \supset \ldots$$

e $\forall i \geq 1$ vale $\pi^i\mathcal{O}_K/\pi^{i+1}\mathcal{O}_K \cong \overline{K}$.
Vale inoltre la seguente proposizione:

Proposizione 1.1. *Sia K un campo completo rispetto ad una valutazione v_K; $\forall i \in \mathbb{Z}$ sia π_i un elemento di K tale che $v_K(\pi_i) = i$; allora la mappa:*

$$Rep : (\overline{K})_{-\infty}^{+\infty} \longrightarrow K \quad (a_i)_{i\in\mathbb{Z}} \mapsto \sum_{-\infty}^{+\infty} rep(a_i)\pi_i$$

è bigettiva. Inoltre, se $(a_i)_{i\in\mathbb{Z}} \neq (0)_{i\in\mathbb{Z}}$ si ha che $v(Rep(a_i)) = min\{i : \ a_i \neq 0\}$.

Una dimostrazione di tale proposizione si può trovare su [FeV]. Utilizzando la proposizione segue facilmente il corollario:

Corollario 1.2. *Prendiamo* $\forall n > 1\ \pi_n = \pi^n$*; allora ogni elemento* $\alpha \in \overline{K}$ *può essere espresso in modo unico come*

$$\alpha = \sum_{-\infty}^{+\infty} \theta_i \pi^i, \quad \text{con } \theta_i \in R \text{ e } \theta_i = 0 \text{ per quasi ogni } i < 0.$$

Definizione 1.2. Se $a - b \in \pi^n \mathcal{O}_K$ scriviamo $a \equiv b\ (mod\ \pi^n)$.

Definiamo ora una filtrazione del gruppo U_K degli elementi invertibili di $\mathcal{O}_K$ nel modo seguente:

$U_K^0 = U_K$;

$U_K^i = \{\ x \in \mathcal{O}_K \mid x \equiv 1\ mod(\pi^i)\ \}$;

Valgono allora le proprietà seguenti di facile dimostrazione:

Proposizione 1.3.

- $U_K/U_K^1 \cong \overline{K}^{\,*}$ *e l'isomorfismo è indotto dalla mappa canonica*

$$\mathcal{O}_K \longrightarrow \mathcal{O}_K/\mathcal{M}_K = \overline{K};$$

- $\forall i \geq 1\ U_K^i/U_K^{i+1}$ *è canonicamente isomorfo a* $\mathcal{M}_K^i/\mathcal{M}_K^{i+1}$ *tramite l'isomorfismo:*

$$U_K^i/U_K^{i+1} \longrightarrow \mathcal{M}_K^i/\mathcal{M}_K^{i+1}$$

$$\overline{x} \longmapsto \overline{x} - 1$$

e $\mathcal{M}_K^i/\mathcal{M}_K^{i+1}$ *è isomorfo (in modo non canonico) al gruppo additivo del campo residuo* $\overline{K}$*.*

Indichiamo per brevità con $U^i = U_K^i$.
Dalle proprietà precedenti segue facilmente il corollario:

Corollario 1.4. *Sia* l *un intero non divisibile per* $p = char\overline{K}$*; allora elevare alla* l *induce un automorfismo di* $U^i/U^{i+1}\ \forall i \geq 1$*. Inoltre, se* K *è completo allora* $\forall i \geq 1$ *il gruppo* U^i *è* l*-divisibile.*

Notiamo che $p = 0$ nel campo dei residui $\overline{K}$ (in quanto stiamo supponendo che $char\overline{K} = p$); si ha quindi che $p \in \mathcal{M}_K$ e quindi $v_K(p) = e \geq 1$.

Definizione 1.3. Tale intero $e = v_K(p)$ è detto indice di ramificazione assoluto di K e si indica con e_K.

Sia π un uniformizzante di K, R un insieme di rappresentanti (come definito precedentemente) e sia $\overline{\theta}_0 \in \overline{K}$ l'elemento di $\overline{K}$ univocamente determinato tramite la relazione $p - rep(\overline{\theta}_0)\pi^e \in \pi^{e+1}\mathcal{O}_K$ (tramite il corollario 1.2). Vale allora la seguente proposizione:

Proposizione 1.5. *Sia K un campo completo rispetto ad una valutazione discreta v_K con $charK = 0$ e $char\overline{K} = p$.*
$\forall i \geq 1$ indichiamo con $\lambda_i : U^i/U^{i+1} \to \overline{K}$ l'omomorfismo definito nella proposizione 1.3. Allora elevare alla p mappa U^i in U^{pi} se $i \leq e/(p-1)$ e U^i in U^{i+e} se $i > e/(p-1)$.
Tale omomorfismo induce i seguenti diagrammi commutativi:

1. *Se $i < e/(p-1)$, vale:*

$$\begin{array}{ccc} U^i/U^{i+1} & \xrightarrow{\hat{}\,p} & U^{pi}/U^{pi+1} \\ \downarrow{\scriptstyle \lambda_i} & & \downarrow{\scriptstyle \lambda_{pi}} \\ \overline{K} & \xrightarrow{\overline{\alpha}\mapsto\overline{\alpha}^p} & \overline{K} \end{array}$$

2. *Se $i = e/(p-1)$ ùn intero, vale:*

$$\begin{array}{ccc} U^i/U^{i+1} & \xrightarrow{\hat{}\,p} & U^{pi}/U^{pi+1} \\ \downarrow{\scriptstyle \lambda_i} & & \downarrow{\scriptstyle \lambda_{pi}} \\ \overline{K} & \xrightarrow{\overline{\alpha}\mapsto\overline{\alpha}^p+\overline{\theta}_0\overline{\alpha}} & \overline{K} \end{array}$$

3. *Se $i > e/(p-1)$, vale:*

$$\begin{array}{ccc} U^i/U^{i+1} & \xrightarrow{\hat{}\,p} & U^{i+e}/U^{i+e+1} \\ \downarrow{\scriptstyle \lambda_i} & & \downarrow{\scriptstyle \lambda_{i+e}} \\ \overline{K} & \xrightarrow{\overline{\alpha}\mapsto\overline{\theta}_0\overline{\alpha}} & \overline{K} \end{array}$$

Gli omomorfismi orizzontali sono iniettivi nei casi (1) e (3) e surgettivi nel caso (3).
In aggiunta se una radice p-esima primitiva dell'unità ζ_p è contenuta in K allora $v_K(1-\zeta_p) = e/(p-1)$ e il nucleo degli omomorfismi orizzontali nel caso (2) sono di ordine p.
Se inoltre $e/(p-1) \in \mathbb{Z}$, $U^{pe/(p-1)+1} \subset (U^{e/(p-1)+1})^p$ e K^* non ha parte di p-torsione, allora l'omomorfismo è iniettivo nel caso (2).

Notiamo infatti che, se $1+\alpha \in U^i$, possiamo scrivere:

$$(1+\alpha)^p = 1 + p\alpha + \frac{p(p-1)}{2}\alpha^2 + \ldots + p\alpha^{p-1} + \alpha^p.$$

Calcoliamo le valutazioni dei vari fattori:

- $v_K(p\alpha) = e + i$;
- $v_K\left(\frac{p(p-1)}{2}\alpha^2\right) = e + 2i$;

$\vdots$

- $v_K(p\alpha^{p-1}) = e + (p-1)i$;
- $v_K(\alpha^p) = pi$.

Di conseguenza otteniamo:

- $v_K((1+\alpha)^p - 1) = v_K(\alpha^p + p\alpha)$, se $v_K(\alpha^p) \neq v_K(p\alpha)$ e
- $v_K((1+\alpha)^p - 1) \geq v_K(\alpha^p + p\alpha)$ altrimenti.

Tali formule descrivono il comportamento dell'elevamento alla p sulla filtrazione di U^1, in quanto $v_K(\alpha^p) \leq v_K(p\alpha) \iff i \leq e/(p-1)$.
Il resto della proposizione si dimostra con opportuni calcoli dello stesso tipo; per ulteriori dettagli si veda [FeV].

Da tale proposizione discendono banalmente i due corollari:

Corollario 1.6. *Sia $charK = 0$ e $\overline{K}$ un campo perfetto di caratteristica $p > 0$; allora*

- $\hat{}^p$ *manda in modo isomorfo U^i/U^{i+1} in U^{pi}/U^{pi+1} se $1 \leq i < e/(p-1)$;*
- $\hat{}^p$ *manda in modo isomorfo U^i/U^{i+1} in U^{i+e}/U^{i+e+1} se $i > e/(p-1)$.*

Corollario 1.7. *Sia K un campo completo e sia $i > pe/(p-1)$; allora si ha $U^i \subset (U^{i-e})^p$. Inoltre, se K^* non contiene radici p-esime primitive dell'unità allora $U^i \subset (U^{i-e})^p \ \forall i \geq pe/(p-1)$.*

1.2 Il gruppo delle unità come $\mathbb{Z}_p$-modulo

Vogliamo studiare la struttura di $\mathbb{Z}_p$-modulo del gruppo delle unità U_K^1 di un campo K completo rispetto ad una valutazione discreta v_K con caratteristica 0 e campo dei residui $\overline{K}$ di caratteristica $p > 0$.

Sia $a = \sum_i a_i p^i$ un elemento di $\mathbb{Z}_p$. Definiamo allora $\varepsilon_n = \varepsilon^{a_0+\ldots+a_n p^n}$.
Notiamo che, se $\varepsilon \in U_K^1$ allora $\varepsilon^{p^n} \to 1$ per $n \to +\infty$. Ciò ci permette di definire

$$\varepsilon^a = \lim_{n\to+\infty} \varepsilon_n.$$

Vale allora il seguente lemma di facile dimostrazione:

Lemma 1.8. *Sia $\varepsilon \in U_K^1$ e $a \in \mathbb{Z}_p$. Allora $\varepsilon^a \in U_k^1$ è ben definito e*

$$\varepsilon^{a+b} = \varepsilon^a\varepsilon^b,\ \varepsilon^{ab} = (\varepsilon^a)^b \text{ e } (\varepsilon\eta)a = \varepsilon^a\eta^a \quad \text{per } \varepsilon.\eta \in U_K^1,\ a, b \in \mathbb{Z}_p.$$

Il gruppo moltiplicativo U_K^1 è uno $\mathbb{Z}_p$-modulo rispetto all'operazione di elevamento a potenza. Inoltre, la struttura dello $\mathbb{Z}_p$-modulo U_K^1 è compatibile con le topologie di $\mathbb{Z}_p$ e di U_K^1.

Consideriamo ora l'omomorfismo:

$$\begin{aligned} \psi : \overline{K} &\longrightarrow \overline{K} \\ \overline{\alpha} &\longmapsto \overline{\alpha}^p + \overline{\theta_0}\ \overline{\alpha} \end{aligned}$$

definito al punto (2) della proposizione 1.5. Supponiamo che una radice p-esima primitiva dell'unità ζ_p appartenga a K e che

$$\zeta_p \equiv 1 + rep(\overline{\theta}_1)\pi^{e/(p-1)} \quad (\pi^{e/(p-1)+1})$$

in quanto sappiamo che $v_K(\zeta_p - 1) = e/(p-1)$. Poiché $\overline{\theta}_1 \in ker\psi$, si ha che $\psi(\overline{\alpha}) = \overline{\theta}_1(\eta^p - \eta)$ con $\eta = \overline{\alpha}\overline{\theta}_1^{-1}$. In generale l'omomorfismo $\eta \to \eta^p - \eta$ si indica solitamente con $\mathcal{P}$. Con tale terminologia si ha che $\psi(\overline{K}) = \overline{\theta}_1{}^p\mathcal{P}(\overline{K})$.
Notiamo inoltre che, se $\overline{K}$ è finito, allora $\overline{K}$ è uno spazio vettoriale su $\mathbb{F}_p$ di dimensione finita, quindi le cardinalità di $ker\psi$ e di $coker\psi$ coincidono. In questo caso allora abbiamo facilemente che $\overline{K} = \psi(\overline{K})$ se e solo se $\overline{K}^*$ non ha parte di torsione e $\psi(\overline{K})$ è di indice p in $\overline{K}$ se e solo se $\zeta_p \in K^*$.

Vale allora il seguente teorema:

Teorema 1.9. *Sia K un campo di caratteristica 0 con campo dei residui perfetto di caratteristica p. $\forall i$ sia π_i l'elemento definito come nella proposizione 1.1. Se $e = v_K(p)$ è divisibile per $p-1$ sia $\psi : \overline{K} \to \overline{K}$ l'omomorfismo definito precedentemente.*
Sia R un insieme di rappresentanti e siano R_0 un sottoinsieme di R tale che i residui dei suoi elementi siano una base di $\overline{K}$ come spazio vettoriale su $\mathbb{F}_p$ e R_0' un sottoinsieme di R tale che i residui dei suoi elementi siano dei generatori di $\overline{K}/\psi(\overline{K})$. Indichiamo con J e J' gli insiemi degli indici rispettivamente di R_0 e di R_0'.Poniamo

$$I = \{i \in \mathbb{Z} \mid 1 \leq i < pe/(p-1),\ (i,p) = 1\}.$$

Indichiamo con v_p la valutazione p-adica.
Allora ogni elemento $\alpha \in U_K^1$ può essere rappresentato come il seguente prodotto convergente

$$\alpha = \prod_{i \in I} \prod_{j \in J} (1 + \theta_j \pi_i)^{a_{ij}} \prod_{j \in J'} (1 + \eta_j \pi_{pe/(p-1)})^{a_j}$$

dove $\theta_j \in R_0$, $\eta_j \in R_0'$, $a_{ij}, a_j \in \mathbb{Z}_p$ (il secondo prodotto compare soltanto se $e/(p-1)$ è un intero) e gli insiemi

$$J_{i,c} = \{j \in J \mid v_p(a_{ij}) \leq c\} \quad e \quad J_c' = \{j \in J' \mid v_p(a_j) \leq c\}$$

sono finiti per ogni $c \geq 0$ e $i \in I$.

Diamo un'idea della dimostrazione.

Dimostrazione. Per dimostrare il teorema mostriamo come ottenere la forma richiesta per $\varepsilon \in U_K^n$ modulo U_K^{n+1}. Se $n = e/(p-1)$ poniamo $\pi_n = \pi^n$.
Sia $\varepsilon = 1 + \theta\pi_n \bmod U_K^{n+1}$ con $\theta \in R$. Dobbiamo distinguere quattro casi:

- Supponiamo $n \in I$. Possiamo trovare $\theta_1, \dots \theta_m \in R_0$ e $b_1, \dots, b_m \in \mathbb{Z}$ che soddisfino la congruenza:

$$1 + \theta\pi_n \equiv \prod_{k=1}^{m} (1 + \theta_k \pi_n)^{b_k} \mod U_K^{n+1} \text{ per qualche } m.$$

- Supponiamo $n < pe/(p-1)$ e $n = p^s n'$ con $n' \in I$. Utilizzando i corollari 1.4 e 1.6 si vede facilmente che esistono $\theta_1, \dots \theta_m \in R_0$ e $b_1, \dots, b_m \in \mathbb{Z}$ tali che

$$1 + \theta\pi_n \equiv \prod_{k=1}^{m} (1 + \theta_k \pi_{n'})^{p^s b_k} \mod U_K^{n+1} \text{ per qualche } m.$$

- Supponiamo $e/(p-1) \in \mathbb{Z}$ e $n = pe/(p-1)$. Usando il punto (2) della proposizione 1.5, il corollario 1.4 e la definizione di R_0' si ha che, se $n = p^s n'$ con $n' \in I$ allora esistono $\theta_1, \dots \theta_m \in R_0$, $\eta_1, \dots, \eta_r \in R_0'$ e $b_1, \dots, b_m,\ c_1, \dots, c_r \in \mathbb{Z}$ tali che

$$1 + \theta\pi_n \equiv \prod_{k=1}^{m}(1+\theta_k\pi_{n'})^{p^s b_k} \prod_{l=1}^{r}(1+\eta_l\pi_n)^{c_l} \mod U_K^{n+1} \text{ per qualche } m, r.$$

- Supponiamo $n > pe/(p-1)$. Usando la proposizione 1.5 e il corollario 1.6 si ha che, se $d' = min\{d \mid n - de \leq pe/(p-1)\}$ e $n' = n - d'e$, allora

$$1 + \theta\pi_n \equiv (1+\theta'\pi_{n'})^{p^d} \mod U_K^{n+1} \text{ per qualche } \theta' \in R.$$

  D'altra parte $n' \leq pe/(p-1)$ quindi possiamo applicare uno dei tre casi precedenti a $1 + \theta'\pi_{n'}$ possiamo scrivere $1 + \theta\pi_n$ nella forma richiesta.

□

Da tale teorema segue l'importante corollario:

Corollario 1.10. *Sia K un campo completo di caratteristica 0 con campo dei residui perfetto di caratteristica p.*

1. *Se K non contiene radici p-esime dell'unità allora la rappresentazione del teorema precedente è unica. Di conseguenza gli elementi del teorema precedente formano una base topologica di U_K^1.*
2. *Se K contiene radici p-esime dell'unità non banali denotiamo con s il massimo intero tale che $\zeta_{p^s} \in K$. Allora gli elementi a_{ij}, a_i del teorema precedente sono univocamente determinati modulo p^s. Di conseguenza gli elementi del teorema formano una base topologica di $U_K^1/(U_K^1)^{p^s}$.*
3. *Se il campo dei residui di K è finito allora U_K^1 è la somma diretta di uno $\mathbb{Z}_p$-modulo libero di rango ef ed una parte di torsione.*

Una dimostrazione di tale corollario può essere trovata su [FeV].

Osservazione 1.11. Dal punto 3. del corollario si vede che nel caso in cui $\overline{K}$ è finito si ha che $U_K^1 \cong \mathbb{Z}_p^n + < \zeta_{p^s} >$, dove $n = [K : \mathbb{Q}_p]$. Se $\{u_1, \dots, u_{n+1}\}$ è un sistema di generatori di U_K^1 e $\zeta_{p^s} = u_1^{a_1} \dots u_{n+1}^{a_{n+1}}$, allora l'unica relazione di dipendenza lineare è

$$1 = (u_1^{a_1} u_2^{a_2} \dots u_{n+1}^{a_{n+1}})^{p^s}.$$

Tale proprietà ci sarà molto utile nella costruzione del capitolo 7.

1.3 Estensioni finite di campi completi

Sia inoltre L un'estensione finita e separabile di K e denotiamo con $\mathcal{O}_L$ la chiusura integrale di $\mathcal{O}_K$ in L. Vale allora il seguente risultato:

Proposizione 1.12. *Nelle ipotesi precedenti, $\mathcal{O}_L$ è un anello di valutazione discreta ed è un modulo libero di rango $n = [L : K]$; inoltre, L è completo rispetto alla topologia definita da $\mathcal{O}_L$.*

Una dimostrazione di tale risultato può essere trovata su [Ser].

Definiamo v_L, $\mathcal{M}_L$, U_L e $\overline{L}$ come nella sezione precedente. In questo capitolo assumiamo che l'estensione dei campi residui $\overline{L}/\overline{K}$ sia separabile (tale condizione è sempre vera quando si trattano i campi p-adici in quanto i campi residui sono finiti).

Definizione 1.4.

- Sia $\mathcal{M}_K\mathcal{O}_L$ l'estensione di $\mathcal{M}_K$ in $\mathcal{O}_L$; allora

$$\mathcal{M}_K\mathcal{O}_L = \mathcal{M}_L{}^e$$

  per qualche $e \in \mathbb{N}$. Tale e è detto indice di ramificazione di L/K e si indica con $e_{L/K}$.

- Il grado dell'estensione dei campi residui $[\overline{L} : \overline{K}]$ è detto grado di inerzia e si indica con $f_{L/K}$.

Vale allora che $n = [L : K] = e_{L/K} f_{L/K}$.

Osservazione 1.13. Notiamo che, se L è completo rispetto alla valutazione discreta v_L allora l'indice di ramificazione assoluto e_L è dato da:

$$e_L = v_L(p) = e_{L/K} e_K.$$

Dalla definizione di indici di ramificazione e gruppi di inerzia discende facilmente la seguente proposizione:

Proposizione 1.14. *Gli indici di ramificazione e i gradi di inerzia sono moltiplicativi sulle torri di estensioni. Più precisamente se $K \subset F \subset L$ sono campi completi rispetto ad una qualche valutazione discreta allora valgono:*

- $e_{L/K} = e_{L/F} e_{F/K}$;
- $f_{L/K} = f_{L/F} f_{F/K}$.

Definizione 1.5.

- Un'estensione L/K si dice non ramificata se $e_{L/K} = 1$; si dice invece totalmente ramificata se $f_{L/K} = 1$;
- Un'estensione L/K con $p = char\overline{K}$ si dice tame se $p \nmid e_{L/K}$;
- Un'estensione L/K con $p = char\overline{K}$ si dice wild se $p \mid e_{L/K}$.

Dalla moltiplicatività degli indici di ramificazione e dei gradi di inerzia sulle torri di estensioni segue direttamente la seguente proposizione:

Proposizione 1.15. *Siano $L \supset F \supset K$ estensioni di campi p-adici; allora:*

1. *L/K non ramificata $\iff$ L/F e F/K non ramificate.*
2. *L/K totalmente ramificata $\iff$ L/F e F/K totalmente ramificate.*

Per le estensioni non ramificate valgono anche le seguenti proprietà (che saranno utili in seguito):

Proposizione 1.16.

1. *Siano L/K e M/K estensioni di campi p-adici; se L/K è non ramificata e M/K è finita allora LM/M è non ramificata.*
2. *Sia K un campo p-adico e denotiamo con K' la sua chiusura algebrica. Allora esiste una corrispondenza biunivoca tra:*

   $$\{L \subset K' \mid L/K \ finita \ e \ non \ ramificata\} \longleftrightarrow \{\overline{L} \subset \overline{K}\,' \mid \overline{L}/\overline{K} \ finita\}$$

Due dimostrazioni delle proprietà precedenti possono essere trovate rispettivamente su [La1] e su [Ser].

1.4 Gruppi di ramificazione

Supponiamo ora che l'estensione L/K sia anche di Galois e indichiamo con G il suo gruppo di Galois. Notiamo che G agisce in modo ovvio su $\mathcal{O}_L$. Vale allora banalmente il seguente lemma:

Lemma 1.17. *Siano $\sigma \in G$ e $i \geq -1$; allora le seguenti condizioni sono equivalenti:*

1. *σ agisce banalmente su $\mathcal{O}_L/{\mathcal{M}_L}^{i+1}$;*
2. *$v_L(\sigma(\alpha) - \alpha) \geq i+1 \quad \forall \alpha \in \mathcal{O}_L$;*
3. *$v_L(\sigma(x) - x) \geq i+1$ dove x è tale che $\mathcal{O}_L = \mathcal{O}_K[x]$.*

Definizione 1.6. $\forall i \geq -1$ definiamo l'i-esimo gruppo di ramificazione:

$$G_i = \{\sigma \in G \mid v_L(\sigma(x) - x) \geq i+1 \text{ con } x \text{ generatore di } \mathcal{O}_L\}$$

Dal lemma precedente si vede che se $\sigma \in G_i$ allora soddisfa anche le condizioni equivalenti (1) e (2).

Osservazione 1.18. Per i gruppi di ramificazione valgono le seguenti proprietà:

1. $\forall i \geq -1$ $G_i \lhd G$ (segue direttamente dalla condizione (1));
2. $G_{i+1} \subset G_i$;
3. $G_i = 1$ definitivamente
   (infatti se $i \geq max_{\sigma \neq id}\{v_L(\sigma(x) - x)\}$ allora $G_i = \{1\}$);
4. G_0 = gruppo di inerzia e $G_{-1} = G$.

I gruppi di ramificazione costituiscono quindi una successione decrescente di sottogruppi normali di G.

Indichiamo nuovamente con x un generatore di $\mathcal{O}_L$ come $\mathcal{O}_K$-algebra; definiamo allora una funzione i_G su G tramite al seguente formula:

$$i_G(s) = v_L(s(x) - x).$$

La funzione i_G ha le seguenti proprietà:

- $i_G(1) = +\infty$ (perché per convenzione si pone $v_L(0) = +\infty$);
- se $s \neq 1$, $i_G(s)$ è un intero non negativo;

- $i_G(tst^{-1}) = i_G(s)$ (perché i G_i sono sottogruppi normali);
- $i_G(s) \geq i+1 \iff s \in G_i$ (che è ovvio dalla definizione di G_i);
- $i_G(st) \geq min\{i_G(s),\ i_G(t)\}$.

Vogliamo ora studiare il comportamento dei gruppi di ramificazione dei sottogruppi di G.
Sia $H < G$ e sia $K' = L^H$ la sottoestensione di L fissata da H; allora dalla corrispondenza di Galois sappiamo che $H = Gal(L/K')$.

$$\begin{array}{c} L \\ | \ H \\ K' \\ | \\ K \end{array}$$

Dalle proprietà viste finora discende facilmente la proposizione seguente:

Proposizione 1.19.
$\forall s \in H$ si ha $i_H(s) = i_G(s)$; di conseguenza $H_i = G_i \bigcap H$.

Ciò mostra che i gruppi di ramificazione di un sottogruppo H di G dipendono direttamente da quelli di G.
Da tale proposizione discende il corollario:

Corollario 1.20. *Sia K_r la massima sottoestensione di L non ramificata su K; allora $K_r = L^{G_0}$ e i gruppi di ramificazione di L/K_r coincidono con quelli di L/K di indici maggiori o uguali a 0.*

Osservazione 1.21. L'estensione L/K_r è totalmente ramificata; per il corollario precedente possiamo quindi ridurre lo studio dei gruppi di ramificazione con indici maggiori e uguali a 0 al caso di estensioni totalmente ramificate.

Supponiamo ora che $H \lhd G$; sempre per la corrispondenza di Galois possiamo identificare G/H con $Gal(K'/K)$.
Abbiamo visto che i gruppi di ramificazione di G determinano quelli di H; per quanto riguarda G/H vale invece la proposizione seguente:

Proposizione 1.22. $\forall \sigma \in G/H$

$$i_{G/H}(\sigma) = \frac{1}{e'} \sum_{s \in \sigma H} i_G(s) \quad con\ e' = e_{L/K'}.$$

Una dimostrazione di tale proposizione può essere trovata su [Ser]; da ciò discende facilmente il seguente corollario:

Corollario 1.23. *Se $H = G_j$ per qualche $j \geq 0$ allora $(G/H)_i = G_i/H$ per $i \leq j$ e $(G/H)_i = 1$ per $i \geq j$.*

1.5 Discriminante e differente

In tale sezione ricordiamo le definizioni di differente e di discriminante di un'estensione di campi; le dimostrazioni delle principali proprietà elencate di seguito possono essere trovate in [La1].

All'interno di questa sezione indichiamo con A un dominio di Dedekind, K il relativo campo dei quozienti, E/K un'estensione finita e separabile di grado $[E : K]$ e B la chiusura integrale di A in E. Sia inoltre $M < (E, +)$ un A-modulo.

Definizione 1.7. Si definisce modulo complementare (o duale) di M l'insieme:

$$M' = \{x \in E \mid Tr(xM) \subset A\}.$$

Valgono allora le seguenti proprietà generali:

- M' è un A-modulo;
- se M è un B-modulo anche M' lo è;
- se M, N sono sottomoduli di E e $M \subset N$ allora $N' \subset M'$;
- se J è un ideale frazionario di B anche J' lo è.

Consideriamo allora il modulo duale di B cioè B'; allora $B \subset B'$, da cui $(B')^{-1} \subset B^{-1} = B$ (perché l'inversione rovescia le inclusioni) e quindi $(B')^{-1}$ è un ideale intero.

Definizione 1.8. Si definisce differente di B/A (o di E/K) l'ideale:

$$\mathcal{D}_{B/A} = (B')^{-1}.$$

Utilizzando le principali proprietà dei moduli complementari si può dimostrare che il differente soddisfa le seguenti proprietà:

- $\mathcal{D}_{B/A}$ è un ideale di B;

- Il differente è moltiplicativo nelle torri di estensioni;
- Se S è un sottoinsieme moltiplicativamente chiuso di A allora:

$$\mathcal{D}_{S^{-1}B/S^{-1}A} = S^{-1}\mathcal{D}_{B/A}$$

- Se E e K sono campi completi e $B = A[\alpha]$ allora

$$\mathcal{D}_{B/A} = (\mu'_\alpha(\alpha))$$

dove μ_α è il polinomio minimo di α su K.

Il differente è uno degli invarianti di un'estensione ed è molto spesso utile per calcolare delle proprietà relative ai gruppi di ramificazione dell'estensione. Vale infatti la seguente proposizione:

Proposizione 1.24. *Nelle ipotesi precendenti vale:*

$$v_L(\mathcal{D}_{L/K}) = \sum_{s \neq id} i_G(s) = \sum_{i \geq 0}(|G_i| - 1)$$

La dimostrazione di tale importante proprietà (che useremo largamente in seguito) si può trovare su [Ser].

Osservazione 1.25. La seconda somma in realtà è finita in quanto abbiamo visto che definitivamente $G_i = \{id\}$ e quindi definitivamente $|G_i| - 1 = 0$.

Siano ora $\sigma_1, \ldots, \sigma_n : E \longrightarrow K'$ n immersioni distinte in una chiusura algebrica K' di K (quindi tali che $\sigma_i|_K = id$) e $W = (w_1, \ldots, w_n)$ un insieme di elementi di E;

Definizione 1.9. Si definisce discriminante di W la seguente quantità:

$$disc_{E/K}(W) = det|\sigma_i(w_j)|^2$$

Osservazione 1.26. Se $V = (v_1, \ldots, v_n)$ è un altro insieme di n elementi di E ed esiste una matrice $X = (x_{ij})$ tale che $W = XV$, allora:

$$discW = (detX)^2\ discV.$$

In più se V e W generano lo stesso modulo su A allora i due discriminanti differiscono per il quadrato di una unità di A.

Proposizione 1.27. *Il discriminante soddisfa le proprietà seguenti:*

- $disc_{E/K}W \subset K$;
- *Se* $W \subset B$ $disc_{E/K}W \subset A$;
- $discW \neq 0 \iff w_1, \ldots, w_n$ *sono linearmente indipendenti su* K.

Definizione 1.10. Sia J un ideale frazionario di E; si definisce discriminante di J la seguente quantità:

$$disc_{E/K}(B) =< disc_{E/K}(W) \mid W = \{w_1, \ldots, w_n\} \subset J \text{ e } W \ K-base \ di \ E > .$$

Definiamo inoltre il discriminante di E/K come:

$$disc(E/K) = disc_{E/K}(B).$$

Proposizione 1.28. *Se* J *è un ideale frazionario di* B *e* $S \subset A$ *è un sottoinsieme moltiplicativamente chiuso, allora:*

$$disc_{E/K}(S^{-1}J) = S^{-1}disc_{E/K}(J).$$

La proposizione precedente ci permette quindi di localizzare per calcolare il discriminante.

Proposizione 1.29. *Supponiamo che* A *sia un anello di Dedekind e* J *un ideale frazionario di* E*; allora:*

$$disc_{E/K}(J) = (N_{E/K}(J))^2 disc_{E/K}(B).$$

Le due precedenti proposizioni combinate insieme permettono di dimostrare facilmente la seguente proposizione:

Proposizione 1.30. *Il discriminante e il differente sono legati insieme dalla formula:*

$$N_{E/K}(\mathcal{D}_{B/A}) = disc_{E/K}(B).$$

1.6 I quozienti G_i/G_{i+1}

Per studiare la filtrazione dei G_i analizziamo il comportamento dei quozienti G_i/G_{i+1}. Indichiamo con π un uniformizzante di L.

Proposizione 1.31. *Sia $i \geq 0$ e $s \in G_0$. Allora:*

$$s \in G_i \quad \Longleftrightarrow \quad \frac{s(\pi)}{\pi} \equiv 1 \mod \mathcal{M}_L^i.$$

Abbiamo infatti visto che a meno di rimpiazzare G con G_0 e K con K_r possiamo supporre che l'estensione sia totalmente ramificata. Allora:

$$i_G(s) = v_L(s(\pi) - \pi) = 1 + v_L(s(\pi)/\pi - 1) \text{ perché } v_L(\pi) = 1,$$

da cui segue la proposizione.

Ritorniamo ora ai gruppi di ramificazione. La proposizione precedente, insieme all'isomorfismo della proposizione 1.3 ci dice che:

$$s \in G_i \quad \Longleftrightarrow \quad s(\pi)/\pi \in U_L^i.$$

Precisamente vale la seguente proposizione:

Proposizione 1.32. *La mappa che assegna ad $s \in G_i$ l'elemento $s(\pi)/\pi$ induce, per passaggio al quoziente, un omomorfismo iniettivo:*

$$\begin{aligned} \vartheta_i : G_i/G_{i+1} &\longrightarrow U_L^i/U_L^{i+1} \\ \overline{s} &\longmapsto \overline{\frac{s(\pi)}{\pi}} \end{aligned}$$

che non dipende dalla scelta dell'uniformizzante π.

Una dimostrazione di tale proposizione può essere trovata in [Ser].
Da tale proposizione discendono alcuni importanti corollari sulla struttura dei G_i:

Corollario 1.33. *G_0/G_1 è un gruppo ciclico e il suo ordine è primo con la caratteristica di $\overline{L}$.*

Dimostrazione. Si ha infatti che

$$G_0/G_1 \cong \theta_0(G_0/G_1) < U^0/U^1 \cong \overline{L}^{\,*}$$

e il gruppo moltiplicativo di un campo è ciclico.
Inoltre $|\overline{L}^{\,*}| = |\overline{L}| - 1$ dunque $|G_0/G_1|$ divide $|\overline{L}^{\,*}|$ che è primo con $char\overline{L}$.

□

Corollario 1.34. *Se* $char\overline{L} = 0$*,* G_0 *è un gruppo ciclico e* G_1 *è banale.*

Dimostrazione. Dalla proposizione 1.32 si ha

$$G_i/G_{i+1} \cong \theta_i(G_i/G_{i+1}) < U_L^i/U_L^{i+1} \cong \overline{L}.$$

Ma, poiché per ipotesi $char\overline{L} = 0$, $\overline{L}$ non ha sottogruppi finiti non banali; di conseguenza $G_i = G_{i+1}$ e poiché $G_i = \{1\}$ definitivamente, si ha $G_1 = \{1\}$.
Allora $G_0/G_1 = G_0$ è ciclico e $G_1 = \{1\}$.

□

Corollario 1.35. *Se* $char\overline{L} = p \neq 0$*,* $\forall i \geq 1$ G_i/G_{i+1} *è un p-gruppo abeliano elementare e* G_1 *è un p-gruppo.*

Dimostrazione. Sappiamo che G_i/G_{i+1} è isomorfo ad un sottogruppo di $\overline{L}$ che è uno spazio vettoriale su $\mathbb{F}_p$; di conseguenza G_i/G_{i+1} è esso stesso uno spazio vettoriale su $\mathbb{F}_p$; ne segue quindi che G_i/G_{i+1} è un p-gruppo abeliano elementare $\forall i$.
Inoltre

$$|G_1| = \prod_{i\geq 1} |G_i/G_{i+1}| \text{ è una potenza di } p$$

quindi G_1 è un p-gruppo.

□

Corollario 1.36. *Sia* K *un campo p-adico e* L/K *un'estensione di Galois. Scriviamo* $[L : K] = fe_0p^s$ *con* $(e_0, p) = 1$*. Allora* $L^{G_0} = K_r$ *e* $L^{G_1} = K_T$*, dove indichiamo con* K_r *e con* K_T *rispettivamente la massima sottoestensione non ramificata e la massima sottoestensione tame di* L/K*.*

Dimostrazione.

$$\begin{array}{c} L \\ {\scriptstyle p^s}\,\big| \\ K_T \\ {\scriptstyle e_0}\,\big| \\ K_r \\ {\scriptstyle f}\,\big| \\ K \end{array}$$

Abbiamo visto precedentemente che $L^{G_0} = K_r$.
Sia K_T la massima sottoestensione tame di L; un'estensione non ramificata è in particolare un'estensione tame e dunque $K_T \supseteq K_r$. Notiamo inoltre che

$|G_0| = e_0 p^s$ e dal corollario 1.34 G_0/G_1 è ciclico e il suo ordine è coprimo con p; di conseguenza $|G_0/G_1|$ divide e_0. D'altra parte dal corollario 1.35 G_1 è un p-gruppo, da cui $|G_0/G_1| = e_0$; allora $[G_0 : G_1] = [L^{G_1} : K_r] = e_0$ e $[L : L^{G_1}] = p^s$. Si ha quindi che L^{G_1} è la massima sottoestensione tame.

□

Corollario 1.37. *Supponiamo char$\overline{L} = p$; allora G_0 è prodotto semidiretto di un sottogruppo ciclico di ordine $e_0 = |G_0/G_1|$ e un sottogruppo normale di ordine $p^n = |G_1|$.*

Dimostrazione. Usiamo il lemma di Zassenhaus:

Lemma 1.38. *Se $N \lhd G$ e $(|N|, |G/N|) = 1$ allora $G \cong N \rtimes H$, con $H \cong G/N$.*

Una dimostrazione di tale classico lemma di teoria dei gruppi può essere trovata su [AlB].

Cerchiamo allora N e H con queste proprietà.
Sia s_0 un elemento di G_0 tale che $< \overline{s}_0 >= G_0/G_1$. Poiché $(e_0, p) = 1 \ \exists \ N > 0$ tale che $p^N \equiv 1 \ (e_0)$. A meno di sostituire N con un suo multiplo possiamo supporre $N > n$ in modo tale che, posto $t = s_0^{p^N}$ allora $t^{e_0} = 1$.
Poiché $p^N \equiv 1 \ (e_0)$ si vede che la proiezione di t in G_0/G_1 è uguale a quella di s; ne segue che il sottogruppo H di G_0 generato da t è ciclico di ordine e_0 e si proietta in modo isomorfo su G_0/G_1.
Allora $|H| = |G_0/G_1| = e_0$, $|G_1| = p^n$, $G_1 \lhd G_0$ e $(e_0, p) = 1$; di conseguenza applicando il lemma otteniamo $G_0 \cong G_1 \rtimes H$.

□

Corollario 1.39. *G_0 è risolubile e, se $\overline{L}$ è finito, anche G è risolubile.*

Dimostrazione. Osserviamo che:
- $G_i \lhd G \ \forall \ i \geq 1$;
- $G_0 \supseteq G_1 \supseteq \ldots \supseteq G_n = \{1\}$.

Inoltre il corollario 1.35 mostra che $\forall \ i \ G_i/G_{i+1}$ è un p-gruppo abeliano elementare; di conseguenza G_0 è risolubile.
La seconda affermazione segue dal fatto che, se $\overline{K}$ è finito, $G/G_0 = Gal(\overline{L}/\overline{K})$ è ciclico, e quindi la catena si prolunga a

$$G \supseteq G_0 \supseteq G_1 \supseteq \ldots \supseteq G_n = \{1\}.$$

□

Le proposizioni seguenti possono essere dimostrate con le stesse tecniche utilizzate finora; ulteriori dettagli si possono trovare su [Ser].
Per la funzione θ_i vale anche la seguente proposizione:

Proposizione 1.40.
Sia ϑ_i l'applicazione definita precedentemente da:

$$\vartheta_i : G_i/G_{i+1} \longrightarrow U_L^i/U_L^{i+1} \cong \mathcal{M}_L^i/\mathcal{M}_L^{i+1}$$
$$\overline{s} \longmapsto \overline{\frac{s(\pi)}{\pi}} \longrightarrow \overline{\frac{s(\pi)}{\pi}} - 1$$

Allora se $s \in G_0$ e $t \in G_i/G_{i+1}$ con $i \geq 1$ si ha:

$$\vartheta_i(sts^{-1}) = \vartheta_0(s)^i \vartheta_i(t).$$

Da tale proposizione discendono banalmente i due corollari seguenti:

Corollario 1.41. *Siano $s \in G_0$ e $t \in G_i$ con $i \geq 1$; allora $sts^{-1}t^{-1} \in G_{i+1} \iff s^i \in G_1$ oppure $t \in G_{i+1}$.*

Corollario 1.42. *Siano G abeliano e $e_0 = |G_0/G_1|$; allora $\forall i \geq 0$ tale che $e_0 \nmid i$ si ha $G_i = G_{i+1}$.*

Con le stesse tecniche si può dimostrare anche il seguente lemma:

Lemma 1.43. *Se $s \in G_i$ e $t \in G_j$ con $i, j \geq 1$ allora $sts^{-1}t^{-1} \in G_{i+1}$ e*

$$\vartheta_{i+j}(sts^{-1}t^{-1}) = (j-i)\vartheta_i(s)\vartheta_j(t).$$

Utilizzando tale lemma si possono dimostrare anche le due importanti proposizioni seguenti:

Proposizione 1.44.
Gli interi tali che $G_i \neq G_{i+1}$ sono congrui modulo $p = char\overline{K}$.

Proposizione 1.45. *Supponiamo che $s \in G_i$ e $t \in G_j$ con $i, j \geq 1$; allora $sts^{-1}t^{-1} \in G_{i+j+1}$.*

1.7 Le funzioni φ e ψ

Sia L/K un'estensione di Galois.

Definizione 1.11. Sia u un numero reale ≥ 1; allora definiamo

$$G_u =: G_i \quad \text{con } i = \lceil u \rceil$$

dove con $\lceil u \rceil$ indichiamo la parte intera superiore di u.

Osserviamo banalmente che con tale definizione si estende la relazione per cui:

$$s \in G_u \quad \Longleftrightarrow \quad i_G(s) \geq u + 1.$$

Poniamo $\forall u \geq -1$

$$\varphi_{L/K}(u) = \varphi(u) = \int_0^u \frac{dt}{[G_0 : G_t]} = \int_0^u \frac{|G_t|}{|G_0|}\, dt$$

con la convenzione che, se $-1 \leq t \leq 0$ allora

- $(G_0 : G_t) = (G_{-1} : G_0)^{-1}$ se $t = -1$;
- $(G_0 : G_t) = (G_0 : G_0)^{-1}$ se $-1 < t \leq 0$.

Notiamo quindi che se $-1 \leq u \leq 0$ allora $\varphi(u) = u$.
Inoltre, se $m \leq u \leq m + 1$ con m intero positivo e $|G_i| = g_i$, si ha:

$$\varphi(u) = \frac{1}{g_0}\,(g_1 + g_2 + \ldots + g_m + (u - m)g_{m+1}).$$

Di conseguenza, se conosciamo la successione degli indici di ramificazione possiamo calcolare anche la φ.
Molte volte è utile considerare:

$$\varphi(u) + 1 = \frac{1}{g_0} \sum_{i=0}^{m} g_i.$$

La funzione φ soddisfa banalmente le seguenti proprietà:

1. φ è continua, lineare a tratti, crescente e concava;
2. $\varphi(0) = 0$;
3. Se indichiamo con φ'_- e con φ'_+ rispettivamente le derivate sinistra e destra de φ allora:

- $\varphi'_-(u) = \varphi'_+(u) = \dfrac{1}{[G_0 : G_u]}$ se $u \notin \mathbb{Z}$;
- $\varphi'_-(m) = \dfrac{1}{[G_0 : G_m]}$ e $\varphi'_+(m) = \dfrac{1}{[G_0 : G_{m+1}]}$ se $m \in \mathbb{Z}$

Sia inoltre $\psi = \psi_{L/K}$ la funzione inversa di φ. Valgono allora le proprietà seguenti:

1. ψ è continua, lineare a tratti, crescente e convessa;
2. $\psi(0) = 0$;
3. Se $v = \varphi(u)$ allora $\psi'_-(v) = \dfrac{1}{\varphi'_-(u)}$ e $\psi'_+(v) = \dfrac{1}{\varphi'_+(u)}$;
4. Se $v \in \mathbb{Z}$ allora $\psi(v) \in \mathbb{Z}$.

Proposizione 1.46. *Dalla definizione di ψ si ha:*

$$\psi(v) = \int_0^v [G^0 : G^w]\, dw.$$

Possiamo ora dare la definizione di gruppi di ramificazione con indice in alto:

Definizione 1.12. Definiamo la successione di gruppi di ramificazione con indice in alto come:

$$G^v := G_{\psi(v)} \ \forall v \geq -1 \quad \text{o equivalentemente} \quad G^{\varphi(u)} := G_u.$$

Per i gruppi di ramificazione in alto valgono facilmente le seguenti proprietà:

- $G^{-1} = G_{\psi(-1)} = G$;
- $G^0 = G_{\psi(0)} = G_0$;
- $G^v = \{e\}$ per v sufficientemente grande.

Vogliamo ora vedere come sono fatti i gruppi di ramificazione con indice in alto delle sottoestensioni.

Sia L/K un'estensione con gruppo di Galois $G = Gal(L/K)$; sia inoltre $H \lhd G$ e $K' = L^H$ la sottoestensione fissata da H.

$$\begin{array}{c} L \\ | \; H \\ K' \\ | \; G/H \\ K \end{array}$$

Enunciamo inizialmente i tre lemmi seguenti:

Lemma 1.47. $\forall u \geq 0$ *vale:*

$$\varphi_{L/K}(u) = \frac{1}{g_0} \sum_{s \in G} inf(i_G(s), u+1) \; - 1.$$

Lemma 1.48. *Sia* $\sigma \in G/H$ *e poniamo* $j(\sigma) = max\{i_G(s) \; : \; s \in \sigma H\}$. *Allora:*

$$i_{G/H}(\sigma) - 1 = \varphi(j(\sigma) - 1).$$

(Tali lemmi sono risutati classici; le relative dimostrazioni possono essere trovate su [Ser]).

Lemma 1.49 (Teorema di Herbrand)**.**
Se $v = \varphi_{L/K'}(u)$ *allora*

$$G_u H/H = (G/H)_v.$$

Dimostrazione. Notiamo che $\sigma \in G_u H/H$ se e solo se $\exists \; s \in G_u$ tale che $\sigma \in sH$, cioè se e solo se $\exists \; s$ tale che $i_G(s) \geq u+1$ e $\sigma \in sH$ se e solo se $j(\sigma) = max\{i_G(s) \mid s \in \sigma H\} \geq u+1$, cioè se e solo se $j(\sigma) - 1 \geq u$.
D'altra parte dalle proprietà precedenti φ è crescente, quindi otteniamo $\varphi_{L/K'}(j(\sigma) - 1) \geq \varphi_{L/K'}(u) = v$.
Ma dal lemma precedente $i_{G/H}(\sigma) - 1 = \varphi_{L/K'}(j(\sigma) - 1) \geq v$, da cui si ha $i_{G/H}(\sigma) \geq v + 1$ e ciò vale se e solo se $\sigma \in (G/H)_v$, da cui la tesi.

□

Grazie a questi lemmi possiamo dimostrare le due proposizioni seguenti che ci serviranno in seguito:

Proposizione 1.50. *Siano* $H \lhd G$ *e* $L^H = K'$*; allora valgono le proprietà seguenti:*

- $\varphi_{L/K} = \varphi_{K'/K} \circ \varphi_{L/K'}$;
- $\psi_{L/K} = \psi_{L/K'} \circ \psi_{K'/K}$.

Dimostrazione.

- Notiamo che l'applicazione $\varphi_{K'/K} \circ \varphi_{L/K'}$ è continua, lineare a tratti e $\varphi(0) = 0$; per dimostrare l'uguaglianza con la funzione $\varphi_{L/K}$ basta dimostrare l'uguaglianza sulle derivate.
  Per le proprietà di composizione vale:

  $$(\varphi_{K'/K} \circ \varphi_{L/K'})'(u) = \varphi'_{K'/K}(v)\varphi'_{L/K'}(u) \quad \text{dove } v = \varphi_{L/K'}(u)$$

  da cui:

  $$(\varphi_{K'/K} \circ \varphi_{L/K'})'(u) = \frac{|(G/H)_v|}{|(G/H)_0|} \frac{|H_u|}{|H_0|}$$
  $$= \frac{1}{e_{K'/K}} \frac{1}{e_{L/K'}} \left(|(G/H)_v| \, |H_u| \right) = \frac{1}{e_{L/K}} \left(|(G/H)_v| \, |H_u| \right);$$

  Ma:

  $$|(G/H)_v| = |G_u H/H| = \frac{|G_u| \, |H|}{|G_u \cap H|} \frac{1}{|H|} = \frac{|G_u|}{|H_u|}$$

  dunque sostituendo si ha:

  $$(\varphi_{K'/K} \circ \varphi_{L/K'})'(u) = \frac{1}{e_{L/K}} \left(\frac{|G_u|}{|H_u|} |H_u| \right) = \frac{|G_u|}{|G_0|} = \varphi'_{L/K}(u)$$

  e quindi le due funzioni coincidono.

- Con lo stesso ragionamento precedente notiamo che $\psi_{L/K'} \circ \psi_{K'/K}$ è continua, lineare a tratti e in 0 vale 0. Osserviamo inoltre che:

  $$(\psi_{L/K'} \circ \psi_{K'/K})(v) = (\varphi^{-1}_{L/K'} \circ \varphi^{-1}_{K'/K})(v)$$
  $$= (\varphi_{K'/K} \circ \varphi_{L/K'})^{-1}(v) = \psi_{L/K}(v)$$

  dunque vale anche l'altra uguaglianza.

□

Proposizione 1.51. *Sia $H \lhd G$; allora $\forall v \geq -1$ vale che:*

$$(G/H)^v = G^v H/H.$$

Dimostrazione.
Per definizione sappiamo che $(G/H)^v = (G/H)_x$ con $x = \psi_{K'/K}(v)$, dove $K' = L^H$.
Dal teorema di Herbrand si ha

$$(G/H)_x = G_u H/H \quad \text{con } u \text{ tale che} \quad x = \varphi_{L/K'}(u).$$

Ora, poiché $x = \varphi_{L/K'}(u)$, si ha $u = \psi_{L/K'}(x)$, con $x \in K'$. Sappiamo inoltre che $x = \psi_{K'/K}(v)$, dunque dalla proposizione precedente otteniamo che:

$$u = \psi_{L/K'}(x) = \psi_{L/K'} \circ \psi_{K'/K}(v) = \psi_{L/K}(v).$$

Di conseguenza, per come sono definiti i gruppi di ramificazione con indice in alto, $G_u = G^v$, da cui:

$$(G/H)^v = (G/H)_x = G_u H/H = G^v H/H.$$

□

Capitolo 2

La norma

2.1 Proprietà della norma

Sia K un campo completo rispetto ad una valutazione discreta v_K; sia L/K un'estensione di Galois e supponiamo che l'estensione dei campi residui $\overline{L}/\overline{K}$ sia separabile.
Ricordiamo la definizione di norma di un'estensione:

Definizione 2.1. Supponiamo che $n = [L : K]$ e siano $\sigma_1 \dots \sigma_n$ gli automorfismi dell'estensione. $\forall x \in L$ definiamo:

$$N_{L/K}(x) = \prod_{i=1}^{n} \sigma_i(x).$$

Osserviamo che d'ora in poi se possibile denoteremo per brevità la norma di un'estensione L/K semplicemente con N.

La norma è un omomorfismo del gruppo moltiplicativo L^* di L nel gruppo moltiplicativo K^*; inoltre essa mappa U_L in U_K, e $v_K(N(x)) = f v_L(x)$, dove $f = [\overline{L} : \overline{K}]$. Di conseguenza vale banalmente il seguente diagramma commutativo:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_L & \longrightarrow & L^* & \xrightarrow{v_L} & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle f} & & \\ 0 & \longrightarrow & U_K & \longrightarrow & K^* & \xrightarrow{v_K} & \mathbb{Z} & \longrightarrow & 0 \end{array}$$

Vogliamo ora descrivere gli effetti principali della norma N sulla filtrazione degli U_L^n (rispettivamente degli U_K^n); molti di questi risultati saranno poi utili per descrivere il comportamento dei salti della ramificazione.

Enunciamo per prima cosa un paio di lemmi tecnici che ci serviranno in seguito; le dimostrazioni di questi due lemmi possono essere reperite su [Ser] e su [Bou].

Lemma 2.1. *Sia*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A' & \longrightarrow & A & \longrightarrow & A'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & & \\ 0 & \longrightarrow & B' & \longrightarrow & B & \longrightarrow & B'' & \longrightarrow & 0 \end{array}$$

un diagramma commutativo con righe esatte. Allora la seguente successione esatta:

$$0 \to Kerf' \longrightarrow Kerf \longrightarrow Kerf'' \longrightarrow Cokerf' \longrightarrow Cokerf \longrightarrow Cokerf'' \to 0$$

è esatta.

Lemma 2.2. *Sia A (rispettivamente A') un gruppo abeliano dotato di una successione decrescente di sottogruppi A_n (rispettivamente A'_n). Supponiamo che $A_0 = A$, $A'_0 = A'$ e che A e A' siano spazi di Hausdorff completi rispetto alla topologia definita dagli A_n e dagli A'_n. Sia $u : A \longrightarrow A'$ un omomorfismo che manda A_n in A'_n $\forall n$. Se gli omomorfismi*

$$u_n : A_n/A_{n+1} \longrightarrow A'_n/A'_{n+1}$$

sono iniettivi per ogni n (rispettivamente surgettivi), allora lo è anche u.

Anche se in seguito ci occuperemo soprattutto del caso di estensioni cicliche e totalmente ramificate, enunciamo rapidamente le proprietà che valgono per le estensioni non ramificate; per ulteriori dettagli si può vedere [Ser].

2.2 Estensioni non ramificate

Indichiamo con $N = N_{L/K}$.

Proposizione 2.3. *Se L/K è non ramificata allora N mappa U_L^n in U_K^n per ogni n.*

Tale proposizione ci dice che che la norma N induce per passaggio al quoziente la mappa seguente:

$$N_n : U_L^n/U_L^{n+1} \longrightarrow U_K^n/U_K^{n+1}.$$

Vale inoltre la proposizione seguente:

Proposizione 2.4. *Se L/K è un'estensione non ramificata allora valgono le seguenti proprietà:*

1. $N(U_L^n) = U_K^n \ \forall n \geq 1$;
2. U_K/NU_L *è isomorfo a* $\overline{K}^*/N\overline{L}^*$;
3. K^*/NL^* *è isomorfo a* $\mathbb{Z}/f\mathbb{Z} \times \overline{K}^*/N\overline{L}^*$.

Da tale proposizione discende banalmente il seguente corollario:

Corollario 2.5. *Le tre condizioni seguenti sono equivalenti:*

1. $(K^* : NL^*) = f$;
2. $U_K = NU_L$;
3. $\overline{K}^* = N\overline{L}^*$.

Osservazione 2.6. Si può dimostrare che la condizione (3) del corollario è soddisfatta quando $\overline{K}$ è un campo finito (che è il caso a cui ci restringeremo in seguito), dunque valgono automaticamente anche le altre due.
Infatti ,se $\overline{K}$ è finito, $\overline{K} = \mathbb{F}_q$ con $q = p^h$ per qualche $h \geq 1$ e $\overline{L} = \mathbb{F}_{q^f}$. Ricordiamo che il gruppo moltiplicativo di un campo finito è ciclico, di conseguenza esiste α tale che $< \alpha >= \mathbb{F}_{q^f}^*$. Ma

$$N_{\mathbb{F}_{q^f}/\mathbb{F}_q}(\alpha) = \alpha^{(q^f-1)/(q-1)}$$

e $< \alpha^{(q^f-1)/(q-1)} >= \mathbb{F}_q^*$, quindi la norma in questo caso è surgettiva.

Analizziamo ora il caso delle estensioni totalmente ramificate; per fare ciò iniziamo con il considerare il caso particolare di estensioni cicliche e totalmente ramificate di grado primo.

2.3 Estensioni cicliche totalmente ramificate di grado primo

Sia L/K un'estensione ciclica e totalmente ramificata di grado $[L : K] = l$; indichiamo con $p = char\overline{K}$. Sappiamo che $G = Gal(L/K) \cong \mathbb{Z}/l\mathbb{Z}$ e che in questo caso c'è un unico salto della ramificazione; denotiamo tale salto con t.

Vale allora che:

$$\begin{cases} G = G_0 = \ldots = G_t \\ G_{t+1} = \ldots = \{e\} \end{cases}$$

Vogliamo caratterizzare tale t. Sia s un generatore del gruppo di Galois G; dalle proprietà della funzione i_G sappiamo che

$$s \in G_u \quad \Longleftrightarrow \quad i_G(s) \geq u + 1.$$

In particolare, se t è un salto, $G = G_t \neq G_{t+1} = \{e\}$, quindi $\forall s \neq e$ si ha

$$i_G(s) \geq t + 1 \quad e \quad i_G(s) < t + 2.$$

Di conseguenza, se s è un generatore del gruppo di Galois G, $i_G(s) = t + 1$ e quindi si ha $t = i_G(s) - 1$.

Osserviamo che, per il corollario 1.35, G_i/G_{i+1} è un p-gruppo abeliano elementare $\forall i \geq 1$, dove p è la caratteristica del campo residuo; di conseguenza, se $l \neq p$, il salto è necessariamente $t = 0$.
D'altra parte, se $l = p$, dal corollario 1.33 si ha che G_0/G_1 è un gruppo ciclico e il suo ordine è primo con $char\overline{L}$, dunque in questo caso necessariamente $G_0 = G_1$ e quindi $t \neq 0$.
Abbiamo quindi il seguente corollario:

Corollario 2.7. *Se L/K è un'estensione ciclica di grado l, con l primo e $char\overline{K} = p$, allora il salto della ramificazione $t = 0 \iff l \neq p$.*

Vogliamo ora vedere qual è il salto della ramificazione in alto (a partire da quello in basso); per fare ciò calcoliamo $\psi(x)$. Dalla definizione sappiamo che, se $m \leq u \leq m + 1$ con m intero positivo, allora:

$$\psi(x) = \int_0^x [G^0 : G^w]\, dw = g_0 \left(\frac{1}{g_1} + \ldots + \frac{1}{g_m} + (u - m)\frac{1}{g_{m+1}} \right).$$

Di conseguenza si ha:

- Se $x \leq t$ e $m \leq x \leq m + 1$:

$$\psi(x) = l \left(\frac{1}{l}\, m + \frac{1}{l}\, (x - m) \right) = x;$$

- se $x > t$:

$$\psi(x) = l \left(\frac{1}{l}\, t + (x - t) \right) = t + l(x - t).$$

Si vede allora che in questo caso anche il salto della ramificazione in alto è uguale a t.

Vogliamo ora studiare come agisce la norma sugli U_L^i. Dimostriamo prima i seguenti lemmi:

Lemma 2.8.
$\forall n \geq 0\ Tr(\mathcal{M}_L^n) = \mathcal{M}_K^r$, *con* $r = [(m+n)/l]$ *e* $m = (t+1)(l-1)$.
(con $[.]$ *indichiamo la parte intera inferiore).*

Dimostrazione. Poiché la traccia è $\mathcal{O}_K$-lineare, $Tr(\mathcal{M}_L^n)$ è un ideale di $\mathcal{O}_K$. Ricordiamo il seguente risultato generale sul differente (di cui si può trovare una dimostrazione su [Ser] o su [La1]):

Proposizione 2.9. *Siano I e J due ideali frazionari di K e di L. Allora le due proprietà seguenti sono equivalenti:*

- $Tr(J) \subset I$;
- $J \subset I\ \mathcal{D}_{L/K}^{-1}$.

Di conseguenza, se r è un intero, dalla proposizione precedente si ha che

$$Tr(\mathcal{M}_L^n) \subset \mathcal{M}_K^r \quad \Longleftrightarrow \quad \mathcal{M}_L^n \subset \mathcal{M}_K^r\ \mathcal{D}_{L/K}^{-1} = \mathcal{M}_L^{lr-m}$$

cioè se e solo se $r \leq (m+n)/l$, da cui la tesi.

□

Lemma 2.10. *Se $x \in \mathcal{M}_L^n$ allora:*

$$N(1+x) \equiv 1 + Tr(x) + N(x) \quad mod\ (\mathcal{M}_L^{2n}).$$

Dimostrazione.

Chiamiamo $\sigma_1, \ldots \sigma_l$ gli elementi di Gal(L/K); allora dalla definizione di norma e traccia si ha:

$$N(x) = N_{L/K}(x) = \prod_{i=1}^{l} \sigma_i(x) \quad \text{e} \quad Tr(x) = Tr_{L/K}(x) = \sum_{i=1}^{l} \sigma_i(x)$$

Di conseguenza possiamo scrivere:

$$\begin{aligned} N(1+x) &= \prod_{i=1}^{l}(1+\sigma_i(x)) \\ &= 1 + \sum_{i=1}^{l}\sigma_i(x) + \left(\sum_{i=1}^{l}\sigma_i\right)\left(\sum_{j=1}^{l} x\sigma_j(x) + \ldots\right) + \prod_{i=1}^{l}\sigma_i(x) \\ &= 1 + Tr(x) + \left(\sum_{i=1}^{l}\sigma_i\right)\left(\sum_{j=1}^{l} x\sigma_j(x) + \ldots\right) + N(x). \end{aligned}$$

Tuttavia, se chiamiamo

$$\alpha = \sum_{j=1}^{l}(x\sigma_j(x) + \ldots)$$

allora

$$v_L(\alpha) \geq 2v_K(x);$$

di conseguenza otteniamo

$$N(1+x) \equiv 1 + Tr(x) + N(x) \quad mod\ (\mathcal{M}_L^{2n})$$

da cui la tesi. □

A partire da questi due lemmi possiamo dimostrare l'importante proposizione seguente:

Proposizione 2.11. *Se L/K è un'estensione ciclica di grado p, allora $\forall n \geq 0$ con n intero si ha $N(U_L^{\psi(n)}) \subset U_K^n$ e $N(U_L^{\psi(n)+1}) \subset U_K^{n+1}$.*

Dimostrazione. Per dimostrare tale proposizione distinguiamo quattro casi:

- Caso $n = 0$.
  In questo caso è ovvio che $N(U_L) \subset U_K$ e $N(U_L^1) \subset U_K^1$;

- Caso $1 \leq n < t$.
  Poiché per ipotesi $t \geq 1$ per le osservazioni fatte precedentemente si ha che l'estensione è totalmente ramificata e quindi $l = p$. Inoltre, per il calcolo della ψ si ha $\psi(n) = n$.
  Sia $x \in \mathcal{M}_L^n$; allora nel caso di estensioni totalmente ramificate si ha $N(x) \in \mathcal{M}_K^n$ in quanto $v_L = v_K \circ N$. Per il lemma 2.8, $Tr(x) \in \mathcal{M}_K^r$, dove
  $$r = \left[\frac{(t+1)(l-1)+n}{l}\right].$$
  Per ipotesi $t > n$, dunque $t = n + h$ con $h \geq 1$. Sostituendo allora si ha:
  $$r = \left[n + h + 1 - \frac{h+1}{l}\right] = \left[n + (h+1)\frac{l-1}{l}\right] \geq n + 1$$

in quanto $h+1 \geq 2$ e $\dfrac{(l-1)}{l} \geq \dfrac{1}{2}$. Di conseguenza $Tr(x) \in \mathcal{M}_K^{n+1}$.
Con lo stesso conto si ha che, se $x \in \mathcal{M}_L^{2n}$, allora $Tr(x) \in \mathcal{M}_K^r$ con

$$r = \left[\frac{(t+1)(l-1)+2n}{l}\right] \geq \left[\frac{(t+1)(l-1)+n}{l}\right] \geq n+1.$$

Di conseguenza $Tr(\mathcal{M}_L^{2n}) \subset \mathcal{M}_K^{n+1}$.
Ora, dal lemma 2.10 si ha che, se $x \in \mathcal{M}_L^n$

$$N(1+x) \equiv 1 + N(x) \quad mod\ \mathcal{M}_K^{n+1};$$

allora, poiché $N(x) \in \mathcal{M}_K^n$ si ha che N mappa U_L^n in U_K^n e U_L^{n+1} in U_K^{n+1}; in questo caso quindi si ha la tesi.

- Caso $n = t \geq 1$.
  Come nel caso precedente si ha che $l = p$ e $\psi(t) = t$. Anche in questo caso, se $x \in \mathcal{M}_L^{2n}$ allora $Tr(x) \in \mathcal{M}_K^r$ con

$$r = \left[\frac{(t+1)(l-1)+2n}{l}\right] = \left[n+1+\frac{n-1}{l}\right] \geq n+1,$$

da cui

$$N(1+x) \equiv 1 + Tr(x) + N(x) \quad mod\ \mathcal{M}_K^{n+1}.$$

D'altra parte, se $x \in \mathcal{M}_L^n$, sempre per il lemma 2.8, $Tr(x) \in \mathcal{M}_K^r$ con

$$r = \left[\frac{(t+1)(l-1)+n}{l}\right] = r = \left[n+1-\frac{1}{l}\right] = n.$$

Di conseguenza N mappa U_L^n in U_K^n e U_L^{n+1} in U_K^{n+1}.

- Caso $n > t$.
  Dai calcoli fatti precedentemente vale $\psi(n) = t + l(n-t)$. Allora, se $x \in \mathcal{M}_L^{\psi(n)}$, $Tr(x) \in \mathcal{M}_K^r$ con

$$r = \left[\frac{(t+1)(l-1)+\psi(n)}{l}\right] = \left[\frac{(t+1)(l-1)+t+l(n-t)}{l}\right]$$

da cui

$$r = \left[n+\frac{l-1}{l}\right] = n.$$

Inoltre, $N(x) \in \mathcal{M}_K^{\psi(n)} \subseteq \mathcal{M}_K^{n+1}$ e, con gli stessi conti precedenti, anche $Tr(\mathcal{M}_L^{2\psi(n)}) \subset \mathcal{M}_K^{n+1}$. Allora utilizzando il lemma 2.10 si ha che, se $x \in \mathcal{M}_L^{\psi(n)}$,

$$N(1+x) \equiv 1 + Tr(x) + N(x) \quad mod\ \mathcal{M}_K^{2\psi(n)}.$$

Mettendo insieme tutte queste osservazioni e utilizzando la formula precedente si ha che N mappa $U_L^{\psi(n)}$ in U_K^n e $U_L^{\psi(n)+1}$ in U_K^{n+1}, e dunque la tesi.

□

Utilizzando la proposizione precedente si vede che la norma definisce, per passaggio al quoziente, un omomorfismo

$$N_n : U_L^{\psi(n)}/U_L^{\psi(n)+1} \longrightarrow U_K^n/U_K^{n+1}.$$

Con ragionamenti analoghi a quelli usati nella dimostrazione precedente, si può dimostrare anche la seguente proposizione che sarà utile in seguito:

Proposizione 2.12.

- *Per $n = 0$ la mappa $N_0 : \overline{K}^* \longrightarrow \overline{K}^*$ è data da $N_0(\xi) = \xi^l$; inoltre:*
  - *se $t \neq 0$ (dove t è il salto della ramificazione) tale mappa è iniettiva;*
  - *se $t = 0$ il ker della mappa è ciclico di ordine l ed è uguale all'immagine di G tramite la mappa $\vartheta_0 : G \longrightarrow U_L/U_L^1$ definita precedentemente;*
- *Per $1 \leq n < t$ la mappa $N_n : U_L^n/U_L^{n+1} \longrightarrow U_K^n/U_K^{n+1}$ è descritta da $N_n(\xi) = \alpha_n \xi^p$ per qualche $\alpha_n \in \overline{K}^*$ ed è iniettiva;*
- *Per $n = t \geq 1$ la mappa $N_t : {U_L}^t/{U_L}^{t+1} \longrightarrow {U_K}^t/{U_K}^{t+1}$ è descritta da $N_t(\xi) = \alpha\xi^p + \beta\xi$ per qualche $\alpha, \beta \in \overline{K}^*$. Il suo Ker è ciclico di ordine $p = l$ ed è uguale a $\vartheta_t(G)$;*
- *Per $n > t$ la mappa $N_n : U_L^{\psi(n)}/U_L^{\psi(n)+1} \longrightarrow U_K^n/U_K^{n+1}$ è descritta da $N_n(\xi) = \beta_n \xi$ per qualche $\beta_n \in \overline{K}^*$ ed è bigettiva.*

(per una dimostrazione completa di tali proprietà si può consultare [Ser]).

Dalla proposizione precedente discende banalmente il seguente corollario:

Corollario 2.13. *L'omomorfismo N_n è iniettivo per ogni n eccetto che per $n = t$ per cui vale la seguente successione esatta:*

$$0 \longrightarrow G \xrightarrow{\vartheta_t} U_L^t/U_L^{t+1} \xrightarrow{N_t} U_K^t/U_K^{t+1}$$

Se il campo dei residui è perfetto, vale la proposizione (che ci sarà utile in seguito):

Proposizione 2.14. *L'omomorfismo N_n è surgettivo per $n > t$ e, se il campo residuo $\overline{K}$ è perfetto, anche per $n < t$. Inoltre, se $\overline{K}$ è algebricamente chiuso, N_n è surgettivo per ogni n.*

Dimostrazione. Osserviamo che dalla proposizione 2.12 sappiamo che se $n > t$ la mappa N_n è bigettiva, quindi in particolare è surgettiva.
Supponiamo ora che il campo dei residui $\overline{K}$ sia perfetto; dalla proposizione 2.12 sappiamo che:

- per $1 \leq n < t$ la mappa $N_n : U_L^n/U_L^{n+1} \longrightarrow U_K^n/U_K^{n+1}$ è descritta da $N_n(\xi) = \alpha_n \xi^p$ per qualche $\alpha_n \in \overline{K}^*$.

Mostriamo che tale mappa è anche sergettiva.
Sappiamo che $U_K^n/U_K^{n+1} \cong \overline{K}$ e che $\overline{K} = \overline{K}^p$; allora se $\beta \in U_K^n/U_K^{n+1}$ esiste $\gamma \in U_K^n/U_K^{n+1}$ tale che $\gamma^p = \beta$, ed esiste $\delta \in \overline{K}$ tale che $\delta^p = \alpha_n$. Si ha quindi:

$$N_n(\delta^{-1}\gamma) = \alpha_n(\delta^{-1}\gamma)^p = \gamma^p = \beta,$$

da cui, se $n < t$, la mappa N_n è surgettiva.

Supponiamo ora che il campo dei residui $\overline{K}$ sia algebricamente chiuso; lo stesso ragionamento precedente mostra che anche in questo caso, se $n < t$, l'omomorfismo N_n è surgettivo.
Consideriamo ora il caso $n = t$; sempre dalla proposizione 2.12 sappiamo che:

- per $n = t \geq 1$ la mappa $N_t : U_L{}^t/U_L{}^{t+1} \longrightarrow U_K^t/U_K{}^{t+1}$ è descritta da $N_t(\xi) = \alpha\xi^p + \beta\xi$ per qualche $\alpha, \beta \in \overline{K}^*$.

Sia $\gamma \in U_K^t/U_K{}^{t+1} \cong \overline{K}$; allora esiste $\xi \in U_K^t/U_K{}^{t+1}$ tale che $\gamma = \alpha\xi^p + \beta\xi$. Dall'affermazione precedente abbiamo quindi che:

$$N_t(\xi) = \alpha\xi^p + \beta\xi = \gamma,$$

dunque la mappa è surgettiva. □

Corollario 2.15. *Se K è un campo perfetto e L/K è un'estensione totalmente ramificata di grado $l = p$ e il campo dei residui è perfetto allora $\forall 1 \leq i < t$ si ha che $U_K^i = U_K^{i+1} N_{L/K}(U_L^i)$ e $U_K^t/N_{L/K}(U_L^t) \cong \mathbb{Z}/p\mathbb{Z}$.*

Dimostrazione. Abbiamo dimostrato che nel caso in cui $\overline{K}$ è perfetto allora se $1 \leq n < t$ si ha che $N_i : U_L^i/U_L^{i+1} \to U_K^i/U_K^{i+1}$ è un isomorfismo; ciò mostra banalmente che $U_L^i = U_L^{i+1} N_{L/K}(U_L^i)$.

□

Corollario 2.16. *$N(U_L^{\psi(n)}) = U_K^n$ per $n > t$ e $N(U_L^{\psi(n)+1}) = U_K^{n+1}$ per $n \geq t$ e n intero. Inoltre, se $\overline{K}$ è algebricamente chiuso tali uguaglianze valgono per ogni n.*

Dimostrazione. Fissiamo $n \geq 0$; filtriamo $U_L^{\psi(n)}$ tramite gli $U_L^{\psi(m)}$ e U_K^n tramite gli U_K^m. Poiché $\forall m$ si ha che $\psi(m+1) \geq \psi(m) + 1$, vale $U_L^{\psi(m+1)} \subset U_L^{\psi(m)+1}$.
Di conseguenza, componendo la proiezione canonica e l'omomorfismo N_m definito in precedenza otteniamo l'omomorfismo ϕ:

$$\phi : U_L^{\psi(m)}/U_L^{\psi(m+1)} \longrightarrow U_L^{\psi(m)}/U_L^{\psi(m)+1} \xrightarrow{N_m} U_K^m/U_K^{m+1} .$$

Se $m > t$, la proposizione 2.14 mostra che ϕ è surgettivo (perché composizione di omomorfismi surgettivi), e applicando il lemma 2.2 si ha quindi che anche l'omomorfismo $N : U_L^{\psi(n)} \longrightarrow U_K^n$ è surgettivo.
Lo stesso ragionamento precedente si applica nel caso in cui $\overline{K}$ è algebricamente chiuso e n è arbitrario (in quanto la proposizione 2.14 afferma che $\forall n \geq 0$ l'omomorfismo N_n è surgettivo).
Per dimostrare la formula $N(U_L^{\psi(n)+1}) = U_K^{n+1}$ notiamo che, da quanto visto al punto precedente, $N(U_L^{\psi(n+1)}) = U_K^{n+1}$. Inoltre dalla proposizione 2.11 si ha che $N(U_L^{\psi(n)+1}) \subset U_K^{n+1}$, quindi:

$$U_K^{n+1} = N(U_L^{\psi(n+1)}) \subset N(U_L^{\psi(n)+1}) \subset U_K^{n+1}$$

da cui l'uguaglianza.

□

Corollario 2.17. *Se $t = 0$ vale che $coker(N_t) = \overline{K}^*/\overline{K}^{*l}$. Se $t \neq 0$, allora $coker(N_t) \cong \overline{K}/\mathcal{P}(\overline{K})$, dove $\mathcal{P}(\xi) = \xi^p - \xi$ è l'omomorfismo definito nel capitolo 1.*

Dimostrazione. Osserviamo che, se $t = 0$ abbiamo visto nella proposizione 2.12 che $N_t(\xi) = \xi^l$, da cui banalmente segue che $coker(N_t) = \overline{K}^*/\overline{K}^{*l}$. Se $t \neq 0$, mostriamo che $coker(N_t) \cong \overline{K}/\mathcal{P}(\overline{K})$. Dalla proposizione 2.12 si ha che

$$N_t(\xi) = \alpha\xi^p + \beta\xi \quad \text{con } \alpha, \beta \neq 0$$

ed esiste un elemento $\eta \in ker N_t$. Possiamo allora scrivere

$$N_t(\xi) = \alpha\eta^p((\xi/\eta)^p - \xi/\eta) = \gamma\mathcal{P}(\xi/\eta) \quad (\gamma \neq 0),$$

da cui $Im(N_t) = \gamma Im(\mathcal{P})$.

□

Corollario 2.18. *Se $\overline{K}$ è perfetto allora $coker(N_t) \cong U_K^t/N(U_L^t)$.*

Dimostrazione. Utilizziamo il seguente diagramma commutativo:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_L^{t+1} & \longrightarrow & U_L^t & \xrightarrow{v_L} & U_L^t/U_L^{t+1} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle N_t} & & \\ 0 & \longrightarrow & U_K^{t+1} & \longrightarrow & U_K^t & \xrightarrow{v_K} & U_K^t/U_K^{t+1} & \longrightarrow & 0 \end{array}$$

e applichiamo il lemma 2.1; poiché $N(U_L^{t+1}) = U_K^{t+1}$ si ha la seguente successione esatta:

$$0 \longrightarrow CokerN \longrightarrow CokerN_t \longrightarrow 0,$$

da cui $U_K^t/N(U_L^t) \cong cokerN_t$.

□

Corollario 2.19. *Se $\overline{K}$ è perfetto si ha che*

$$U_K/N(U_L) \cong K^*/NL^*.$$

Dimostrazione. Utilizziamo il seguente diagramma commutativo:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_L & \longrightarrow & L^* & \xrightarrow{v_L} & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle \cdot f} & & \\ 0 & \longrightarrow & U_K & \longrightarrow & K^* & \xrightarrow{v_K} & \mathbb{Z} & \longrightarrow & 0 \end{array}$$

e applichiamo il lemma 2.1; osserviamo che nel nostro caso, essendo l'estensione totalmente ramificata, $f = 1$, da cui $f'' = id$ e $Kerf'' = Cokerf'' = 0$. Di conseguenza dal lemma si ha:

$$0 \longrightarrow Cokerf' \longrightarrow Cokerf \longrightarrow 0,$$

e quindi, poiché $Cokerf' = U_K/NU_L$ e $Cokerf = K^*/NL^*$ vale

$$U_K/NU_L \cong K^*/NL^*.$$

□

Per dimostrare risultati analoghi nel caso generale di estensioni totalmente ramificate di grado qualsiasi abbiamo bisogno di un altro strumento; nel prossimo paragrafo definiamo i polinomi additivi e moltiplicativi enunciandone alcune proprietà.

2.4 Polinomi additivi e polinomi moltiplicativi

Sia K un campo e indichiamo con p la sua caratteristica.

Definizione 2.2. Un polinomio $P \in K[x]$ si dice moltiplicativo se

$$P(XY) = P(X)P(Y) \quad e \quad P(1) = 1.$$

Per i polinomi moltiplicativi valgono banalmente le proprietà seguenti:

- Un polinomio moltiplicativo è necessariamente un monomio del tipo X^h; indichiamo con $d(P)$ il grado h.
- Se h è della forma $h_0 p^r$, con $(h_0, p) = 1$, si definisce h_0 grado separabile di P, e scriviamo $d_s(P) = h_0$.
- Il nucleo dell'omomorfismo $P : K^* \longrightarrow K^*$ è il gruppo delle radici $d_s(P)$-esime dell'unità contenute in K; l'ordine di questo gruppo divide $d_s(P)$.
- Se P e Q sono due polinomi moltiplicativi lo è anche $P \circ Q$ e

$$d(P \circ Q) = d(P) \cdot d(Q), \quad d_s(P \circ Q) = d_s(P) \cdot d_s(Q).$$

Definizione 2.3. Un polinomio P è detto additivo se:

$$P(X + Y) = P(X) + P(Y).$$

Per i polinomi additivi valgono invece le proprietà seguenti:

- Se K ha caratteristica zero allora $P(X) = aX$ per qualche $a \in K$; se invece K ha caratteristica p è evidente che P è combinazione lineare di monomi della forma X^{p^h} con potenze di p come esponenti.
  Se $P \neq 0$ può essere scritto in modo unico nella forma:

$$P = X^{p^h} P'$$

  con

$$P' = a_0 + \ldots + a_k X^{p^k} \quad e \ a_0, a_k \neq 0.$$

- Il grado $d(P)$ di P (scritto nella forma precedente) è uguale a p^{h+k}; l'intero p^k è detto grado separabile di P e si indica con $d_s(P)$.

- Il nucleo dell'omomorfismo $P : K \longrightarrow K$ è uguale a quello di P'; esso è un sottogruppo additivo di K con ordine che divide $d_s(P)$. Inoltre, poiché P' è separabile, esso può essere scritto (nella chiusura algebrica di K) come:
$$P' = a_K \prod_{P(\xi)=0} (X - \xi)$$
che mostra che il Ker di P ha ordine $d_s(P)$ se K contiene le radici di P'.

- Se P e Q sono due polinomi additivi lo è anche $P \circ Q$ e
$$d(P \circ Q) = d(P) \cdot d(Q), \quad d_s(P \circ Q) = d_s(P) \cdot d_s(Q).$$

Utilizzando tali polinomi possiamo generalizzare i risultati sulle estensioni totalmente ramificate di grado primo al caso di estensioni totalmente ramificate di grado qualsiasi.

2.5 Estensioni di Galois totalmente ramificate

In questo paragrafo supponiamo che l'estensione L/K sia di Galois e totalmente ramificata; di conseguenza $\overline{L} = \overline{K}$.
Per prima cosa dimostriamo la seguente proposizione:

Proposizione 2.20. *$\forall n \geq 0$ si ha $N(U_L^{\psi(n)}) \subset U_K^n$ e $N(U_L^{\psi(n)+1}) \subset U_K^{n+1}$.*

Dimostrazione. Vogliamo dimostrare la proposizione per induzione sulla lunghezza della fattorizzazione di $|G|$. Osserviamo innanzitutto che, se $|G| = 1$ non c'è nulla da dimostrare. Supponiamo allora $|G| \neq 1$.

- Passo base: $|G| = l$ con l primo.
Tale caso è esattamente la proposizione 2.11 trattata precedentemente;

- Passo induttivo
Per il corollario 1.39 sappiamo che il gruppo G_0 è risolubile; nel nostro caso, essendo l'estensione totalmente ramificata, si ha che $G = G_0$ (perché il primo salto è diverso da 0); dunque anche G è risolubile. Segue allora che G ha un quoziente ciclico e di ordine primo; di conseguenza

esiste una sottoestensione K'/K di L/K che sia ciclica di grado primo l.

$$\begin{array}{c} L \\ | \\ K' \\ | \ l \\ K \end{array}$$

Applicando l'ipotesi induttiva si ha che le due asserzioni sono valide per entrambe le sottoestensioni L/K' e K'/K. Poniamo:

$$n' = \psi_{K'/K}(n) \quad e \quad n'' = \psi_{L/K'}(n');$$

allora si ha:

$$N_{L/K'}(U_L^{n''}) \subset U_{K'}^{n'} \quad e \quad N_{K'/K}(U_{K'}^{n'}) \subset U_K^n.$$

Applicando la regola di composizione $N_{L/K} = N_{K'/K} \circ N_{L/K'}$, si ha:

$$N_{L/K}(U_L^{n''}) = N_{K'/K}(N_{L/K'}(U_L^{n''})) \subset N_{K'/K}(U_{K'}^{n'}) \subset U_K^n$$

che dimostra la prima affermazione in quanto $\psi_{L/K} = \psi_{L/K'} \circ \psi_{K'/K}$.
Allo stesso modo, sempre per l'ipotesi induttiva, si ha che:

$$N_{L/K'}(U_L^{n''+1}) \subset U_{K'}^{n'+1} \quad e \quad N_{K'/K}(U_{K'}^{n'+1}) \subset U_K^{n+1}$$

dunque componendo le due relazioni si ha

$$N_{L/K}(U_L^{n''+1}) = N_{K'/K}(N_{L/K'}(U_L^{n''+1})) \subset N_{K'/K}(U_{K'}^{n'+1}) \subset U_K^{n+1}.$$

□

Vogliamo ora descrivere la mappa N_n con l'uso dei polinomi moltiplicativi (o additivi). A tal riguardo vale la seguente proposizione:

Proposizione 2.21. *Per $n = 0$ (rispettivamente $n \neq 0$) l'omomorfismo N_n è indotto da un polinomio moltiplicativo (rispettivamente additivo) non costante P_n tale che:*

$$d(P_n) = |G_{\psi(n)}| \quad e \quad d_s(P_n) = [G_{\psi(n)} : G_{\psi(n)+1}] = \psi'_d(n)/\psi'_g(n),$$

dove con f'_d e f'_g indichiamo rispettivamente le derivate prime destra e sinistra di f.
Inoltre la successione

$$0 \longrightarrow G_{\psi(n)}/G_{\psi(n)+1} \xrightarrow{\vartheta} U_L^{\psi(n)}/U_L^{\psi(n)+1} \xrightarrow{N_n} U_K^n/U_K^{n+1}$$

è esatta.

Dimostrazione. Come nella proposizione precedente facciamo la dimostrazione per induzione sulla lunghezza della fattorizzazione di $|G|$. Osserviamo di nuovo che se $|G| = 1$ non c'è nulla da dimostrare; supponiamo quindi $|G| \neq 1$.

- Passo base: $|G| = l$ con l primo.
  Tale caso discende banalmente dalla proposizione 2.12.

- Passo induttivo.
  Con lo stesso ragionamento della dimostrazione della proposizione precedente esiste una sottoestensione K'/K di L/K che sia ciclica di grado primo l.

$$\begin{array}{c} L \\ \Big| \; H \\ K' \\ \Big| \; G/H \\ K \end{array}$$

  Poniamo:

$$n' = \psi_{K'/K}(n) \quad e \quad n'' = \psi_{L/K'}(n');$$

  notiamo che N_n ha la seguente fattorizzazione:

$$U_L^{n''}/U_L^{n''+1} \xrightarrow{N''} U_{K'}^{n'}/U_{K'}^{n'+1} \xrightarrow{N'} U_K^n/U_K^{n+1}$$

  dove con N'' ed N' indichiamo rispettivamente le norme $N_{L/K'}$ e $N_{K'/K}$. Per ipotesi induttiva N'' ed N' sono indotte dai polinomi moltiplicativi (rispettivamente additivi) P'' e P'; allora N_n è indotta dal polinomio composto $P_n = P' \circ P''$ che è dello stesso tipo per le osservazioni precedenti.
  Inoltre, il grado separabile $d_s(P_n)$ è uguale al prodotto dei gradi separabili $d_s(P')$ e $d_s(P'')$. Dall'ipotesi induttiva applicata all'estensione L/K' si ha che

$$d_s(P'') = (\psi_{L/K'})'_{d/g}(n),$$

  dove con $f'_{d/g}$ denotiamo il quoziente f'_d/f'_g delle derivate destra e sinistra di f. Allo stesso modo:

$$d_s(P') = (\psi_{K'/K})'_{d/g}(n).$$

  Poiché $\psi_{L/K} = \psi_{L/K'} \circ \psi_{K'/K}$, dalla regola della catena si ha

$$d_s(P_n) = d_s(P') \cdot d_s(P'') = (\psi_{L/K})'_{d/g}(n).$$

Ora, per le proprietà principali della funzione ψ si ha che:

$$(\psi_{L/K})'_d(n) = [G_0 : G_{\psi(n)}] \quad e \quad (\psi_{L/K})'_g(n) = [G_0 : G_{\psi(n)+1}],$$

da cui:

$$d_s(P_n) = \frac{[G_0 : G_{\psi(n)}]}{[G_0 : G_{\psi(n)+1}]} = [G_{\psi(n)} : G_{\psi(n)+1}].$$

Dimostriamo che il grado di P_n è pari a $|G_{\psi(n)}|$.
Dall'ipotesi induttiva sappiamo che:

$$d(P'') = |H_{\psi_{L/K'}(n')}| \quad e \quad d(P') = |(G/H)_{\psi_{K'/K}(n)}|;$$

inoltre, per il teorema di Herbrand 1.49 si ha che, se $v = \varphi_{L/K'}(u)$ (o equivalentemente se $u = \psi_{L/K'}(v)$),

$$(G/H)_v = G_u H/H = G_{\psi_{L/K'}(v)} H/H.$$

Inoltre abbiamo visto dalla proposizione 1.19 che, per i sottogruppi H di G, vale $H_t = G_t \cap H \ \forall t$.
Dunque, calcolando le cardinalità, si ha:

$$d(P_n) = |(G/H)|_{n'} |H_{\psi_{L/K'}(n')}| = |G_{\psi_{L/K'}(n')} H/H| \cdot |H_{\psi_{L/K'}(n')}|$$

ma $\psi_{L/K'}(n') = n'' = \psi_{L/K}(n)$, dunque sostituendo si ha:

$$\begin{aligned} d(P_n) &= |G_{n''} H/H||H_{n''}| = \frac{|G_{n''} H|}{|H|} |G_{n''} \cap H| \\ &= \frac{|G_{n''}||H|}{|G_{n''} \cap H|} \frac{|G_{n''} \cap H|}{|H|} = |G_{\psi_{L/K}(n)}|. \end{aligned}$$

D'altra parte, per quanto abbiamo visto nella sezione precedente, il nucleo di N_n ha ordine che divide $d_s(P_n)$; poiché $N(s(\pi)/\pi) = 1$, tale nucleo contiene l'immagine di ϑ, il cui ordine è precisamente $d_s(P_n)$ come visto prima. Di conseguenza $Im(\vartheta) = Ker(N_n)$, quindi la successione è esatta.

□

Corollario 2.22. *N_n è iniettiva* $\iff$ $G_{\psi(n)} = G_{\psi(n)+1}$.

Dimostrazione. Segue direttamente dall'esattezza della successione

$$0 \longrightarrow G_{\psi(n)}/G_{\psi(n)+1} \xrightarrow{\vartheta} U_L^{\psi(n)}/U_L^{\psi(n)+1} \xrightarrow{N_n} U_K^n/U_K^{n+1}$$

della proposizione precedente; infatti ϑ è iniettiva e $Im\vartheta = ker N_n$. Di conseguenza $KerN_n = \{0\} \iff Im\vartheta \cong G_{\psi(n)}/G_{\psi(n)+1} = \{0\}$, da cui la tesi.

□

Corollario 2.23. *N_n è surgettiva in ognuno dei tre casi seguenti:*

1. *$\overline{K}$ è algebricamente chiuso:*
2. *$\overline{K}$ è perfetto e $G_{\psi(n)} = G_{\psi(n)+1}$;*
3. *$G_{\psi(n)} = \{1\}$.*

Dimostrazione. Distinguiamo vari casi:

1. Supponiamo che $\overline{K}$ sia algebricamente chiuso. Dalla proposizione 2.21 l'applicazione
$$N_n : U_L^{\psi(n)}/U_L^{\psi(n)+1} \longrightarrow U_K^n/U_K^{n+1}$$
è indotta da un polinomio P_n non costante. Sia allora $\beta \in U_K^n/U_K^{n+1} \cong \overline{K}$; poiché $\overline{K}$ è algebricamente chiuso esiste $x \in \overline{K}$ tale che $P_n(x) = \beta$; di conseguenza:
$$N_n(x) = P_n(x) = \beta,$$
quindi l'applicazione N_n è surgettiva.

2. Supponiamo che $\overline{K}$ sia perfetto e che $G_{\psi(n)} = G_{\psi(n)+1}$. Sempre dalla proposizione 2.21 l'applicazione
$$N_n : U_L^{\psi(n)}/U_L^{\psi(n)+1} \longrightarrow U_K^n/U_K^{n+1}$$
è indotta da un polinomio P_n tale che $d_s(P_n) = [G_{\psi(n)} : G_{\psi(n)+1}] = 1$. Di conseguenza per le proprietà dei polinomi moltiplicativi viste nella sezione precedente si ha che P_n è un monomio di grado una potenza di p, cioè della forma $P_n = cX^{p^r}$ con $c \in \overline{K}$. Sia allora $\beta \in U_K^n/U_K^{n+1} \cong \overline{K}$; poiché $\overline{K}$ è perfetto esiste $b \in \overline{K}$ tale che $b^{p^r} = c$, ed esiste γ tale che $\gamma^{p^r} = \beta$. Di conseguenza:
$$N_n(b^{-1}\gamma) = cb^{-p^r}\gamma^{p^r} = \gamma^{p^r} = \beta,$$
quindi anche in questo caso N_n è surgettiva.

3. Supponiamo che $G_{\psi(n)} = \{1\}$. Utilizzando ancora la proposizione 2.21 l'applicazione
$$N_n : U_L^{\psi(n)}/U_L^{\psi(n)+1} \longrightarrow U_K^n/U_K^{n+1}$$
è indotta da un polinomio P_n tale che $d(P_n) = |G_{\psi(n)}| = 1$. Di conseguenza il polinomio P_n è un monomio di grado 1, cioè della forma $P_n = cX$, con $c \in \overline{K}$. Se consideriamo $\beta \in U_K^n/U_K^{n+1} \cong \overline{K}$, allora
$$N_n(c^{-1}\beta) = cc^{-1}\beta = \beta,$$
dunque N_n è surgettiva anche in questo caso.

□

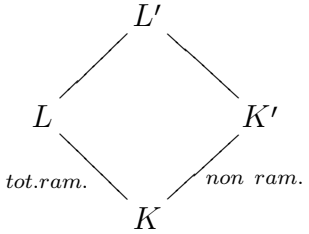
Con la stessa dimostrazione del corollario 2.16 si può dimostrare il seguente corollario:

Corollario 2.24. *Se $G_{\psi(n)} = \{1\}$ vale $N(U_L^{\psi(n)}) = U_K^n$ e se $G_{\psi(n+1)} = \{1\}$ si ha $N(U_L^{\psi(n)+1}) = U_K^{n+1}$. Se $\overline{K}$ è algebricamente chiuso tali uguaglianze valgono $\forall n \geq 0$.*

Utilizzando le proprietà delle norme descritte finora vogliamo dare una dimostrazione dell'importante teorema di Hasse-Arf. Per fare ciò abbiamo bisogno di un'altra osservazione preliminare.

2.6 Estensione del campo dei residui

Sia L/K un'estensione finita totalmente ramificata; supponiamo in aggiunta che il campo dei residui $\overline{L} = \overline{K}$ sia un campo perfetto.
Sia $\overline{K'}$ un'estensione finita di $\overline{K}$ e sia K' la corrispondente estensione di K non ramificata (ottenuta utilizzando la corrispondenza della proposizione 1.15).



Le estensioni L/K e K'/K sono linearmente disgiunte; infatti $L \cap K'$ è un'estensione di K contemporaneamente non ramificata e totalmente ramificata, quindi è banale, e $L \cap K' = K$.

Ora, sempre per la proposizione 1.15 si ha che l'estensione L'/L è non ramificata con estensione del campo dei residui $\overline{K'}/\overline{K}$.

Definizione 2.4. Diciamo che L'/K' è dedotta da L/K tramite estensione dei campi residui da $\overline{K}$ a $\overline{K'}$.

Siano π_K e π_L due uniformizzanti rispettivamente di K ed L; allora, poiché le estensioni K'/K e L'/L sono non ramificate, π_K e π_L sono ancora uniformizzanti rispettivamente di K' e di L'.
Se supponiamo che L/K sia di Galois con gruppo di Galois G, lo stesso vale per L'/K'; inoltre i gruppi di ramificazione di G (e i rispettivi salti) e le funzioni ϑ_i definite in precedenza sono le stesse per L/K e L'/K'.

Tale costruzione ci dice quindi che possiamo, se necessario, estendere il campo dei residui dell'estensione di partenza conservando gli invarianti principali dell'estensione iniziale.

2.7 Applicazione: il teorema di Hasse-Arf

Siamo ora in grado di fornire una dimostrazione completa del teorema di Hasse-Arf.

Teorema 2.25. *Sia K un campo completo rispetto ad una valutazione discreta e sia L un'estensione abeliana finita di K con gruppo di Galois G; supponiamo inoltre che l'estensione dei campi residui $\overline{L}/\overline{K}$ sia separabile. Vale allora che, se v è un salto della filtrazione $\{G^v\}$ di G, v è un intero.*

Tradotto in termini di salti della ramificazione in basso il teorema diventa:

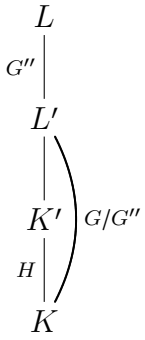
Teorema 2.26. *Nelle ipotesi del teorema precedente, se μ è un intero tale che $G_\mu \neq G_{\mu+1}$ allora $\varphi_{L/K}(\mu)$ è intero.*

La seguente proposizione è un caso speciale del teorema precedente:

Proposizione 2.27. *Sia L/K un'estensione ciclica e totalmente ramificata con gruppo di Galois G e sia μ il più grande intero tale che $G_\mu \neq \{1\}$. Allora $\varphi_{L/K}(\mu)$ è un intero.*

Mostriamo innanzitutto che la proposizione precedente implica il teorema di Hasse-Arf.

Dimostrazione. Sia L/K un'estensione che soddisfi le ipotesi del teorema e sia v un salto nella filtrazione $\{G^v\}$. Abbiamo precedentemente visto che, a meno di rimpiazzare G con il suo sottogruppo di inerzia G_0 possiamo supporre che l'estensione L/K sia totalmente ramificata.
Poniamo $G' = G^v$ e sia G'' il successivo gruppo di ramificazione (dunque $G'' = G^{v+\varepsilon}\ \forall \varepsilon > 0$ sufficientemente piccolo); dalla definizione vale allora che $G' \neq G''$.
Per ipotesi G è abeliano, dunque lo è anche G/G''; di conseguenza, utilizzando il teorema fondamentale dei gruppi abeliani, G/G'' può essere scomposto nel prodotto diretto di gruppi ciclici. Esiste allora un gruppo quoziente H di G/G'' ciclico e tale che l'immagine H' di G' in H sia diversa da $\{1\}$.



Per la corrispondenza di Galois, G/G'' è il gruppo di Galois di una sottoestensione L'/K di L/K, e H è il gruppo di Galois di una sottoestensione K'/K di L'/K.
Indichiamo con $\widetilde{G} = G/G''$; allora per costruzione esiste $\widetilde{H} \lhd \widetilde{G}$ tale che $H = \widetilde{G}/\widetilde{H}$. Utilizzando la proposizione 1.51 si ha che:

$$H^v = (\widetilde{G}/\widetilde{H})^v = \widetilde{G}^v\ \widetilde{H}/\widetilde{H} = (G/G'')^v\ \widetilde{H}/\widetilde{H};$$

d'altra parte per $\widetilde{G}$ si ha:

$$\widetilde{G}^v = (G/G'')^v = G^v\ G''/G'' = G'\ G''/G'' = G'/G'',$$

dunque sostituendo si ha:

$$H^v = G'/G''\ \widetilde{H}/\widetilde{H} = H' \neq 1 \quad \text{per costruzione.}$$

Allo stesso modo calcoliamo $H^{v+\varepsilon}$:

$$H^{v+\varepsilon} = (\widetilde{G}/\widetilde{H})^{v+\varepsilon} = \widetilde{G}^{v+\varepsilon}\ \widetilde{H}/\widetilde{H} = (G/G'')^{v+\varepsilon}\ \widetilde{H}/\widetilde{H};$$

ma

$$\widetilde{G}^{v+\varepsilon} = (G/G'')^{v+\varepsilon} = G^{v+\varepsilon}\ G''/G'' = G''/G'' = \{1\},$$

dunque sostituendo otteniamo:

$$H^{v+\varepsilon} = \widetilde{H}/\widetilde{H} = \{1\}.$$

Abbiamo quindi dimostrato che $H^v = H' \neq \{1\}$ e $H^{v+\varepsilon} = \{1\}$. Utilizzando la proposizione 2.27 si ha che v è un intero, da cui la tesi.

□

Resta da dimostrare la proposizione 2.27.
Denotiamo con v_L la valutazione discreta di L e sia π un uniformizzante di L. Poniamo:

$$r = |G|, \quad r' = |G_\mu| \quad e \quad k = r/r'.$$

Scegliamo un generatore s di G; poiché il gruppo G è ciclico per ipotesi, anche G_μ è ciclico ed è generato da $\sigma = s^k$. A meno di estendere opportunamente i campi come mostrato nella sezione precedente possiamo supporre che il campo dei residui $\overline{L} = \overline{K}$ sia diverso da $\mathbb{F}_p$.

Sia V l'insieme degli $x \in L^*$ di norma 1; d'ora in poi per comodità utilizziamo la notazione esponenziale per il gruppo G (cioè scriviamo x^s al posto di $s(x)$).

Ricordiamo l'enunciato del teorema 90 di Hilbert:

Teorema 2.28 (Teorema 90)**.**
Sia L/K un'estensione ciclica e di Galois e sia α un elemento di L. Allora $N(\alpha) = 1 \iff$ esiste un elemento $\beta \in L$ tale che $\alpha = \beta^{s-1}$, dove s è un generatore di $Gal(L/K)$.

Una dimostrazione di tale teorema (che è un risultato classico di teoria dei campi), può essere trovata su [Bos].

Grazie al teorema 90 si vede che V può essere espresso come

$$V = \{\ y^{s-1} \mid y \in L^*\ e\ < s >= G\ \}.$$

Sia inoltre W il sottogruppo di V definito come:

$$W = \{y^{s-1} \mid y \in U_L \text{ e } < s >= G\}.$$

Vale allora il seguente lemma:

Lemma 2.29. *Il gruppo V/W è ciclico.*

Dimostrazione. Notiamo infatti che la mappa

$$f : G \longrightarrow V/W$$
$$t \longmapsto \pi^{t-1}$$

definisce, per passaggio al quoziente, un isomorfismo tra G e V/W. Di conseguenza V/W è ciclico perché G lo è.

□

Sia ora m un intero non negativo.

Definizione 2.5. Definiamo:

$$V_m = V \cap U_L^m \quad e \quad W_m = W \cap U_L^m.$$

Osserviamo facilmente che, poiché $W \subset V$, anche $W_m \subset V_m$; inoltre i gruppi V_m/W_m possono essere identificati con sottogruppi di V/W ed essi formano una filtrazione decrescente di V/W.

Lemma 2.30. *Per m sufficientemente grande, si ha $V_m = W_m$.*

Dimostrazione. Dall'osservazione precedente vale che $W_m \subset V_m \ \forall m \geq 0$; dimostriamo l'inclusione ooposta. Fissiamo un elemento $t \in L$ on $Tr_{L/K}(t) = 1$ e denotiamo con $m_0 = -v_L(t)$. Sia $x \in V_m$ con $m > m_0$; mostriamo che $x \in W_m$. Consideriamo l'elemento:

$$y = \sum_{i=0}^{r-1} (x^{1+s+\ldots+s^{i-1}} \cdot t^{s^i});$$

poiché per ipotesi $Tr_{L/K}(t) = 1$, possiamo scrivere:

$$y - 1 = \sum_{i=0}^{r-1} (x^{1+s+\ldots+s^{i-1}} \cdot t^{s^i}) - \sum_{i=0}^{r-1} t^{s^i} = \sum_{i=0}^{r-1} (x^{1+s+\ldots+s^{i-1}} - 1) \cdot t^{s^i},$$

da cui $v_L(y-1) > 0$ e $y \in U_L^1$. Poiché per ipotesi $N_{L/K}(x) = 1$ si ha che $y^{1-s} = x$, da cui $x \in W_m$.

□

Studiamo adesso le proprietà dei quozienti successivi $V_m/V_{m+1}W_m$ della filtrazione $\{V_m/W_m\}$.

Lemma 2.31. *Se $\varphi(m)$ è un intero e se $G_m = G_{m+1}$ allora $V_m = V_{m+1}$.*

Dimostrazione. Poniamo $n = \varphi(m)$ in modo che $m = \psi(n)$.
Sia $x \in V_m$ e sia $\overline{x}$ l'immagine di x in U_L^m/U_L^{m+1}. Per definizione di V_m, $N_{L/K}(x) = 1$ dunque $\overline{x}$ appartiene al nucleo dell'omomorfismo:

$$N_n : U_L^m/U_L^{m+1} \longrightarrow U_K^n/U_K^{n+1}$$

definito precedentemente. Tuttavia dalla proposizione 2.21 il nucleo di N_n è isomorfo a G_m/G_{m+1}, che in questo caso è banale per ipotesi. Segue quindi che $\overline{x} = 0$ e dunque $x \in V_{m+1}$.

□

Lemma 2.32. *Sia m un intero positivo. Se l'immagine di W_m in U_L^m/U_L^{m+1} è non banale, allora l'immagine è tutto U_L^m/U_L^{m+1}.*

Dimostrazione. Sia x un elemento di W_m che non appartenga a U_L^{m+1}; allora $x = y^{s-1}$ con $y \in U_L$. A meno di moltiplicare y per un elemento di U_K (che non cambia y^{s-1}) possiamo supporre che $y \in U_L^1$; di conseguenza $y = 1 + z$ con $v_L(z) \geq 1$.
$\forall a \in \mathcal{O}_K$ poniamo $y_a = 1 + az$ e $x_a = y_a^{s-1}$. Allora:

$$x_a - 1 = \frac{s(y_a) - (y_a)}{y_a} = \frac{a(s(y) - y)}{y_a} = a\frac{y}{y_a}\,(x - 1).$$

Poiché $y/y_a \in U_L^1$, si vede che $x_a \in W_m$ e l'immagine $\overline{x}_a$ in U_L^m/U_L^{m+1} è uguale a $\overline{ax}$, dove con $\overline{a}$ denotiamo l'immagine di a nel campo dei residui $\overline{L} = \overline{K}$. Tuttavia, poiché $\overline{x} \neq 0$, ogni elemento di U_L^m/U_L^{m+1} è della forma $\overline{ax}$, dunque l'applicazione è surgettiva.

□

Lemma 2.33. *Sia n un intero tale che $G_{\psi(n+1)} = 1$; sia m un intero tale che*

$$n < \varphi(m) < n + 1;$$

allora, le immagini di V_m e W_m sono entrambe uguali a tutto U_L^m/U_L^{m+1}.

Dimostrazione.

- Mostriamo che l'immagine di V_m è esattamente U_L^m/U_L^{m+1}. Sia $x \in U_L^m$ un rappresentante di $\overline{x} \in U_L^m/U_L^{m+1}$. Per ipotesi

  $$n < \varphi(m) < n + 1, \quad \text{da cui:} \quad \psi(n) < m < \psi(n + 1),$$

  quindi $m \geq \psi(n) + 1$. Dalla proposizione 2.20 si ha che $N_{L/K}(x) \in U_K^{n+1}$ e il corollario 2.24 mostra che $\exists y \in U_L^{\psi(n+1)}$ tale che $N_{L/K}(y) = N_{L/K}(x)$. Poniamo $x' = xy^{-1}$; in questo modo abbiamo ottenuto un rappresentante di $\overline{x}$ che appartiene a V; di conseguenza l'immagine di V_m è tutto U_L^m/U_l^{m+1}.

- Consideriamo ora W_m; la sua immagine in U_L^m/U_L^{m+1} è un sottogruppo che indichiamo con H_m. Per quanto visto in precedenza, V/W è un gruppo ciclico e quindi lo è anche V_m/W_m perché sottogruppo di un gruppo ciclico; di conseguenza il quoziente di U_L^m/U_L^{m+1} tramite H_m è anch'esso un gruppo ciclico.
  Tuttavia U_L^m/U_L^{m+1} è isomorfo al gruppo additivo $\overline{K}$, che non è ciclico in quanto stiamo supponendo $\overline{K} \neq \mathbb{F}_p$. Si ha quindi che $H_m \neq 0$, e il lemma precedente mostra che H_m deve essere l'intero gruppo.

□

Lemma 2.34.
Sia m un intero e n il più piccolo intero che sia maggiore o uguale a $\varphi(m)$. Se $G_{\psi(n+1)} = \{1\}$, allora $V_m = W_m$.

Dimostrazione. Mostriamo per prima cosa che $V_m = V_{m+1}W_m$. Distinguiamo due casi:

- Supponiamo $\varphi(m) \in \mathbb{Z}$; allora $\psi(m) = n+1$ e $\psi(n+1) = m$.
  Poiché $\{1\} = G_m = G_{\psi(n+1)} = G_{m+1}$, per il lemma 2.31 si ha $V_m = V_{m+1}$, e quindi $V_m = V_{m+1}W_m$;

- se $\varphi(m) \notin \mathbb{Z}$ allora $n < \varphi(m) < n+1$ e il lemma precedente mostra che V_m e W_m hanno la stessa immagine in U_L^m/U_L^{m+1}, da cui $V_m = V_{m+1}W_m$.

Applicando lo stesso ragionamento a $m+1$ si ha che $V_{m+1} = V_{m+2}W_{m+1}$, da cui $V_m = V_{m+2}W_m$. Applicando l'induzione otteniamo quindi che $\forall k > 0$ vale $V_m = V_{m+k}W_m$.
Prendendo k abbastanza grande si ha, dal lemma 2.30, $V_{m+k} = W_{m+k}$, quindi

$$V_m = V_{m+k}W_m = W_{m+k}W_m = W_m$$

da cui la tesi. □

Possiamo infine dimostrare la proposizione 2.27.

Dimostrazione. Supponiamo per assurdo che $\varphi(\mu)$ non sia intero e sia $\nu+1$ il più piccolo intero tale che $\nu+1 \geq \varphi(\mu)$.
Abbiamo allora che $\mu < \psi(\nu+1)$, da cui $G_{\psi(\nu+1)} = \{1\}$; utilizzando il lemma precedente si ha dunque $V_\mu = W_\mu$.
Sia $\sigma = s^k$ il generatore di G_μ definito all'inizio e poniamo $x = \pi^{\sigma-1}$.
Osserviamo che $x \in V_\mu$; infatti, se $F = Fix(G_\mu)$ allora, per il teorema 90 di Hilbert si ha che $N_{L/K'}(\pi^{\sigma-1}) = 1$, e quindi dalla composizione delle norme

$$N_{L/K}(\pi^{\sigma-1}) = N_{K'/K}(N_{L/K'}(\pi^{\sigma-1})) = 1,$$

dunque $x \in V$. D'altra parte, se $\sigma \in G_\mu$, si ha $v_L(\sigma(\pi) - \pi) \geq \mu + 1$, e quindi $\pi^{\sigma-1} \in U_L^\mu$; di conseguenza $\pi^{\sigma-1} \in V_\mu$.
Ora, poiché $V_\mu = W_\mu$ esiste $y \in U_L$ tale che $\pi^{\sigma-1} = y^{s-1}$. Ma:

$$\sigma - 1 = (s-1)(1 + s + \ldots + s^{k-1})$$

e, ponendo $z = y^{-1}\pi^{(1+s+\ldots+s^{k-1})}$, si vede che $z^{s-1} = 1$, da cui $z \in K^*$.
Ora, poiché L/K è totalmente ramificata, segue che $v_L(z) \equiv 0 \mod r$ (dove con r indichiamo $[L : K]$). Tuttavia, poiché $v_L(y) = 0$ e $v_L(\pi) = 1$, si ha che $k \equiv 0 \mod r$, il che è assurdo.

□

Esempio 2.1. *Ci sono alcuni casi in cui si dimostra direttamente che i salti della ramificazione in alto sono interi senza utilizzare il teorema di Hasse-Arf.*

- *Se l'estensione L/K è ciclica di grado p, abbiamo visto che il salto in alto coincide con quello in basso (quindi in quarticolare è intero).*
- *Se l'estensione è di Galois di grado p^2, il teorema di Hasse-Arf segue direttamente dalla proposizione 1.44. Infatti, se indichiamo con t_1 e t_2 i salti in basso (eventualmente solo t^1 se l'estensione ha un unico salto) si ha:*
  - *$t^1 = \varphi(t_1) = t_1$, quindi il primo salto in alto è uguale al salto in basso;*
  - *$t^2 = \varphi(t_2) = \frac{1}{p^2}(p^2 t_1 + p(t_2 - t_1) = t_1 + \frac{1}{p}(t_2 - t_1)$; d'altra parte per la proposizione 1.44 si ha che $t_1 \equiv t_2 \ (p)$, quindi $t^2 = t_1 + \frac{1}{p}(t_2 - t_1)$ è intero.*

Concludiamo tale capitolo con tre importanti esempi.

2.8 Esempi:

2.8.1 Estensioni cicliche totalmente ramificate

Sia L/K un'estensione ciclica e totalmente ramificata di grado p^n, con $p = char\overline{K}$; allora $G = \mathbb{Z}/p^n\mathbb{Z}$. Vogliamo descrivere le proprietà generali dei salti della ramificazione in questo caso.
Indichiamo con $G(i)$ il sottogruppo di G di ordine p^{n-i}.

- Poiché $p = char\overline{K}$ abbiamo precedentemente visto che il primo salto è diverso da 0; di conseguenza $G = G_0 = G_1$.
- Per il corollario 1.35 abbiamo visto che G_i/G_{i+1} è un p-gruppo abeliano elementare, ed essendo quoziente di un gruppo ciclico è anch'esso ciclico. Di conseguenza:

  $$|G_i/G_{i+1}| = 1 \ o \ |G_i/G_{i+1}| = p.$$

  Si ha quindi che tutti i sottogruppi di G sono gruppi di ramificazione e la successione dei gruppi di ramificazione diventa:

  $$G = G(0) \supset G(1) \supset \ldots \supset G(n-1) \supset G(n) = \{1\}.$$

Dal teorema di Hasse-Arf sappiamo che esistono degli interi positivi

$$i_0, i_1 \ldots i_{n-1}$$

tali che i salti della ramificazione in alto $\{G^\nu\}$ si abbiano nei punti:

$$i_0, i_0 + i_1, \ \ldots \ , \ i_0 + i_1 + \ldots + i_{n-1}.$$

Da tali valori possiamo allora dedurre i salti della ramificazione in basso:

- Supponiamo che il primo salto in basso si abbia in j_0; allora:

  $$\varphi(j_0) = \frac{g_1}{g_0} + \ldots + \frac{g_{j_0}}{g_0} = j_0$$

  in quanto $\forall i \leq j_0$ vale $\dfrac{g_i}{g_0} = 1$.
  Poiché il primo salto in alto è i_0, si ha $i_0 = j_0$.
- Supponiamo che i_0, $i_0 + l_1$, $\ldots$ siano i salti della ramificazione in basso; allora:

  – $\varphi(i_0 + l_1) = i_0 + \dfrac{1}{p} l_1 \in \mathbb{Z}$; allora

  $$i_0 + \frac{1}{p} l_1 = i_0 + i_1 \quad \Longleftrightarrow \quad l_1 = p i_1.$$

  $\vdots$

  – $\varphi(i_0 + l_1 + \ldots + l_{n-1}) = i_0 + \dfrac{1}{p} p i_1 + \dfrac{1}{p^2} p^2 i_2 + \ldots + \dfrac{1}{p^{n-1}} l_{n-1} \in \mathbb{Z}$; allora

  $$i_0 + i_1 + \ldots + \frac{l_{n-1}}{p^{n-1}} = i_0 + i_1 + \ldots + i_{n-1} \iff l_{n-1} = p^{n-1} i_{n-1}.$$

Vogliamo ora vedere cosa possiamo dire sulle sottoestensioni di L/K.

Sia dunque L/K un'estensione ciclica e totalmente ramificata di grado p^n, con $p = char\overline{K}$. Consideriamo la catena di sottogruppi di ramificazione:

$$G = G_1 \supseteq G_2 \supseteq \ldots \supseteq G_l \supset G_{l+1} = \{1\}.$$

Sia L_m il sottocampo fissato da G_m; allora abbiamo la seguente torre di estensioni:

$$K = L_1 \subseteq L_2 \subseteq \ldots \subseteq L_l \subset L_{l+1} = L.$$

Vale allora la seguente proposizione:

Proposizione 2.35.
Sia $1 \leq m \leq l$; allora $Gal(L_{m+1}/L_m)$ coincide con il gruppo di ramificazione $Gal(L_{m+1}/L_m)_m$, $Gal(L_{m+1}/L_m)_{m+1} = 1$ e $\psi_{L_{m+1}/L_m}(m) = m$.
Inoltre:

- *se $i < m$, allora $\psi_{L_{m+1}/L_m}(i) = i$ e l'omomorfismo*

  $$U^i_{L_{m+1}}/U^{i+1}_{L_{m+1}} \longrightarrow U^i_{L_m}/U^{i+1}_{L_m}$$

  indotto da N_{L_{m+1}/L_m} è iniettivo (bigettivo se il campo dei residui è perfetto);

- *se $i > m$, allora l'omomorfismo*

  $$U^{\psi(i)}_{L_{m+1}}/U^{\psi(i)+1}_{L_{m+1}} \longrightarrow U^i_{L_m}/U^{i+1}_{L_m}$$

  indotto da N_{L_{m+1}/L_m} con $\psi = \psi_{L_{m+1}/L_m}$ è bigettivo;

- *in aggiunta, l'omomorfismo*

  $$U^{\psi(i)}_{L}/U^{\psi(i)+1}_{L} \longrightarrow U^i_{K}/U^{i+1}_{K}$$

  indotto da $N_{L/K}$ con $\psi = \psi_{L/K}$ è bigettivo se $\psi(i) > n$.

Dimostrazione. Dimostriamo la proposizione per induzione su m.

- Passo base $m = l$.
  L'estensione intermedia L/L_l ha grado p e $Gal(L/L_l) = G_l$ per la corrispondenza di Galois. Dalla proposizione 1.19 sappiamo che

  $$Gal(L/L_l)_x = Gal(L/K)_x \cap Gal(L/L_l);$$

allora si vede che

$$Gal(L/L_l)_l = G_L = Gal(L/L_l) \ e \ Gal(L/L_l)_{l+1} = \{1\}$$

e

$$\psi_{L/L_l}(x) = x \text{ per } x \leq l.$$

Le altre asserzioni seguono direttamente dalla proposizione 2.12.

- Passo induttivo $m+1 \to m$.
  Sappiamo che la funzione ψ è moltiplicativa sulle torri di estensioni, quindi:

  $$\psi_{L/L_{m+1}}(x) = \psi_{L/L_l} \circ \psi_{L_l/L_{l-1}} \circ \dots \psi_{L_{m+2}/L_{m+1}}(x) = x \quad \forall x \leq m+1;$$

  ora, per il teorema 1.51, si ha:

  $Gal(L_{m+1}/L_m)_x = Gal(L/L_m)_{\psi_{L/L_{m+1}}(x)} \ Gal(L_{m+1}/L_m)/Gal(L_{m+1}/L_m).$

  Vale quindi:

  - $Gal(L_{m+1}/L_m)_m = Gal(L_{m+1}/L_m)$. Infatti:

    $Gal(L_{m+1}/L_m)_m = Gal(L/L_m)_m \ Gal(L_{m+1}/L_m)/Gal(L_{m+1}/L_m)$

    perché $\psi_{L/L_{m+1}}(m) = m$; d'altra parte:

    $Gal(L/L_m)_m = Gal(L/L_m) \cap Gal(L/K)_m = G_m$

    dunque sostituendo:

    $Gal(L_{m+1}/L_m)_m = G_m/G_{m+1} = Gal(L_{m+1}/L_m).$

  - $Gal(L_{m+1}/L_m)_{m+1} = \{1\}$. Infatti:

    $Gal(L_{m+1}/L_m)_{m+1} = Gal(L/L_m)_{m+1} Gal(L_{m+1}/L_m)/Gal(L_{m+1}/L_m);$

    ma

    $Gal(L/L_{m+1})_{m+1} = Gal(L/K)_{m+1} \cap Gal(L/L_m) = G_{m+1} \cap G_m = G_{m+1},$

    dunque sostituendo si ha:

    $Gal(L_{m+1}/L_m)_{m+1} = G_{m+1}/G_{m+1} = \{1\}.$

  Le altre affermazioni seguono direttamente dalle proposizioni 2.12 e 2.21.

□

2.8.2 Estensioni ciclotomiche di $\mathbb{Q}_p$

Un altro esempio di spiccato interesse è dato dalle estensioni ottenute aggiungendo a $\mathbb{Q}_p$ le radici p^l-esime dell'unità.
Consideriamo $K = \mathbb{Q}_p$ e $K_s = \mathbb{Q}_p(\zeta_{p^s})$; valgono allora le seguenti proprietà:

- $[K_s : K] = \phi(p^s) = p^{s-1}(p-1)$;
- Il gruppo di Galois dell'estensione K_s/K può essere identificato con $\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{s-1}\mathbb{Z}$;
- K_s è un'estensione totalmente ramificata di K; l'elemento $\pi = \zeta - 1$ è un uniformizzante di K_s e $\mathcal{O}_{K_s} = \mathcal{O}_K[\zeta]$.
- Se $s = 1$ l'estensione K_1/K è un'estensione tame; se invece $s > 1$ l'estensione K_s/K_1 è wild.

Vogliamo ora determinare i salti in alto e in basso della ramificazione dell'estensione. $\forall \nu \geq 1$ denotiamo con:

$$G(p^s)^\nu = \{\ x \in (\mathbb{Z}/p^s\mathbb{Z})^* \ :\ x \equiv 1\ (mod\ p^\nu)\}$$

il sottogruppo di $(\mathbb{Z}/p^s\mathbb{Z})^*$ di ordine $p^{n-\nu}$ e indichiamo con $K_{s-\nu}$ il campo fissato da $G(p^s)^\nu$.
Vogliamo dimostrare la seguente proposizione:

Proposizione 2.36. *I gruppi di ramificazione con indice in basso di G sono dati da:*

- $G = G_0$;
- $G_u = G(p^s)^1 \qquad se\ 1 \leq u \leq p-1$;
- $G_u = G(p^s)^2 \qquad se\ p \leq u \leq p^2 - 1$;

$\vdots$

- $G_u = \{1\} \qquad se\ p^{s-1} \leq u$.

I salti in basso della ramificazione sono quindi uguali a $0,\ p-1 \ldots p^{s-1}-1$.

Dimostrazione. Notiamo che $(\mathbb{Z}/p^s\mathbb{Z})^* \cong G$ mediante l'isomorfismo seguente:

$$\begin{aligned}(\mathbb{Z}/p^s\mathbb{Z})^* &\longrightarrow G\\ a &\longmapsto s_a\end{aligned}$$

dove s_a è l'elemento del gruppo di Galois definito da

$$s_a(\zeta) = \zeta^a.$$

Vogliamo mostrare che

$$a \in G(p^s)^\nu \quad \Longleftrightarrow \quad s_a \in G_u \text{ con } u \leq p^\nu - 1.$$

Supponiamo che $a \in G(p^s)^\nu - G(p^s)^{\nu+1}$; allora $a \equiv 1\ (p^\nu)$ e ν è l'intero più grande con questa proprietà.
Dalla definizione di gruppi di ramificazione sappiamo che

$$G_u = \{\sigma \in G \mid v_{K_s}(\sigma(x) - x) \geq u + 1 \text{ con } \mathcal{O}_{K_s} = \mathcal{O}_K[x]\ \}.$$

Per calcolare $i_G(s_a)$ possiamo usare $x = \zeta_{p^s}$:

$$\begin{aligned}i_G(s_a) &= v_{K_s}(s_a(\zeta_{p^s}) - \zeta_{p^s}) = v_{K_s}(\zeta_{p^s}^a - \zeta_{p^s}) = v_{K_s}(\zeta_{p^s}) + v_{K_s}(\zeta_{p^s}^{a-1} - \zeta_{p^s})\\ &= v_{K_s}(\zeta_{p^s}^{a-1} - 1);\end{aligned}$$

d'altra parte, poiché $a \notin G(p^s)^{\nu+1}$ si ha che $\zeta_{p^s}^{a-1}$ è una radice $p^{s-\nu}$-esima primitiva dell'unità, quindi $\zeta_{p^s}^{a-1} = \zeta_{p^{s-\nu}}$ e $\zeta_{p^{s-\nu}} - 1$ è un uniformizzante di $K_{n-\nu}$; di conseguenza:

$$v_{K_s}(\zeta_{p^{s-\nu}} - 1) = e_{K_s/K_{s-\nu}} = p^\nu.$$

Se $p^{k-1} \leq u \leq p^k - 1$ si vede che $s_a \in G_u \iff \nu \geq k$, il che mostra quindi che $G_u = G(p^s)^\nu$.

□

Anche in questo caso si può dimostrare in modo diretto che i salti della ramificazione in alto sono interi; vale allora la seguente proposizione:

Proposizione 2.37. *I salti della filtrazione $\{G^v\}$ sono interi. Più precisamente:*

- $G^v = G(p^s)^{[v]}$ *se* $0 \leq v < s$;
- $G^v = \{1\}$ *se* $v \geq s$.

I salti in alto della ramificazione sono quindi uguali a $0, 1 \ldots, s-1$.

Dimostrazione. Sappiamo che i salti della filtrazione $\{G_u\}$ sono della forma $u = p^k - 1$; calcoliamo dunque $\varphi(p^k - 1)\ \forall 0 \le k \le s$.

- $\varphi(0) = 0$;
- $\varphi(p-1) = \dfrac{g_1}{g_0} + \ldots + \dfrac{g_{p-1}}{g_0}$

  ma $g_1 = \ldots = g_{p-1} = p^{n-1}$ e $g_0 = (p-1)p^{n-1}$, dunque sostituendo si ha:

  $$\varphi(p-1) = \frac{p^{n-1}}{(p-1)p^{n-1}} + \ldots + \frac{p^{n-1}}{(p-1)p^{n-1}} = \frac{p-1}{p-1} = 1.$$

  In generale:

- $\varphi(p^k - 1) = k - 1 + \dfrac{(p^k - 1 - (p^{k-1} - 1))p^{n-k}}{(p-1)p^{n-1}}$

  $= k - 1 + \dfrac{p^{k-1}(p-1)p^{n-k}}{(p-1)p^{n-1}} = k.$

□

2.8.3 Estensioni non abeliane di $\mathbb{Q}_p$

Diamo infine un esempio di estensione di $\mathbb{Q}_p$ che sia non abeliana; in particolare mostriamo che in questo caso i salti in alto della ramificazione possono non essere interi.

In generale le estensioni di questo tipo possono essere abbastanza complicate da trattare; in questo caso ci limitiamo ad enunciare soltanto i risultati fondamentali; per ulteriori dettagli si può consultare [Viv].

Consideriamo le estensioni della forma $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^s]{b})/\mathbb{Q}_p$ con $0 < s \le r$, $p \nmid b$ e $b \in \mathbb{Q}_p - \mathbb{Q}_p^p$. Per tale estensione valgono le seguenti proprietà:

- L'estensione $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^s]{b})/\mathbb{Q}_p$ è totalmente ramificata. Infatti abbiamo già visto nell'esempio precedente che che l'estensione $\mathbb{Q}_p(\zeta_{p^r})/\mathbb{Q}_p$ è totalmente ramificata $\forall r \ge 1$; basta allora dimostrare che anche l'estensione $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^s]{b})/\mathbb{Q}_p(\zeta_{p^r})$ lo è e applicare la proprietà delle torri (la dimostrazione dell'ultima affermazione non è immediata e si può trovare su [Viv]);

- $[\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^s]{b}) : \mathbb{Q}_p] = [\mathbb{Q}_p(\zeta_{p^r}\sqrt[p^s]{b}) : \mathbb{Q}_p(\zeta_{p^r})][\mathbb{Q}_p(\zeta_{p^r}) : \mathbb{Q}_p]$
  $= p^s\varphi(p^r) = p^s p^{r-1}(p-1)$;
- il gruppo di Galois dell'estensione è dato da:

$$Gal(\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^s]{b})/\mathbb{Q}_p) \cong \mathbb{Z}/p^s\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p^r\mathbb{Z}^*$$

  dove il prodotto semidiretto è fatto rispetto alla mappa:

$$\varphi : \mathbb{Z}/p^r\mathbb{Z}^* \twoheadrightarrow \mathbb{Z}/p^s\mathbb{Z}^* \cong Aut(\mathbb{Z}/p^s\mathbb{Z}).$$

Indichiamo con $(\mathbb{Z}/p^r\mathbb{Z}^*)^k = \{\sigma \in \mathbb{Z}/p^r\mathbb{Z}^* \mid v_p(\sigma - 1) \geq k\} \cong \mathbb{Z}/p^{r-k}\mathbb{Z}$.
Si può dimostrare (studiando le varie sottoestensioni a partire da quelle del tipo $\mathbb{Q}_p(\zeta_{p^h})/\mathbb{Q}_p$ viste nell'esempio precedente) che in questo caso i gruppi di ramificazione con indici in alto sono:

1. $G^0 = \mathbb{Z}/p^s\mathbb{Z} \rtimes \mathbb{Z}/p^r\mathbb{Z}^*$
2. $G^{(i-1)+1/(p-1)} = \mathbb{Z}/p^{s-i+1}\mathbb{Z} \rtimes (\mathbb{Z}/p^r\mathbb{Z}^*)^i$
3. $G^i = \mathbb{Z}/p^{s-i}\mathbb{Z} \rtimes (\mathbb{Z}/p^r\mathbb{Z}^*)^i$
4. $G^{s+j} = (\mathbb{Z}/p^r\mathbb{Z}^*)^{s+j}$

con $1 \leq i \leq s$ e $1 \leq j \leq r-1-s$ (con la convenzione che se $r-1 \leq s$ i gruppi di ramificazione del punto 4. non ci sono). Se indichiamo con d^i la differenza tra l'$i+1$-esimo e l'i-esimo salto in alto della ramificazione, allora vale:

- $d^0 = 0$;
- $d^{2i-1} = 1/(p-1)$;
- $d^{2i} = (p-2)/(p-1)$;
- $d^{2s+j} = 1$.

I salti quindi sono:

- $t^1 = 0$;
- $t^2 = t^1 + d^1 = 1/(p-1)$;
- $t^3 = t^2 + d^2 = 1/(p-1) + (p-2)/(p-1) = 1$;

$\vdots$

- $t^{2s} = t^{2s-1} + d^{2s-1} = (s+1) + 1/(p-1) = ((s+1)p - s)/(p-1)$;
- $t^{2s+1} = t^{2s} + d^{2s} = ((s+1)p - s)/(p-1) + (p-2)/(p-1) = s+2$;
- $t^{2s+2} = t^{2s+1} + d^{2s+1} = s+2+1 = s+3$;

$\vdots$

- $t^{2s+(r-s)} = t^{s+r} = t^{s+r-1} + d^{s+r-1} = s + r.$

Si vede quindi che non tutti i salti in alto della ramificazione sono interi.

Possiamo considerare anche le estensioni della forma $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^s]{a})/\mathbb{Q}_p$ con $0 < s \leq r$, $p \parallel a$ e $a \in \mathbb{Q}_p - \mathbb{Q}_p^p$. Anche in questo caso, come prima, l'estensione è totalmente ramificata e il gruppo di Galois è

$$Gal(\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^s]{a})/\mathbb{Q}_p) \cong \mathbb{Z}/p^s\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p^r\mathbb{Z}^*.$$

I gruppi di ramificazione con indici in alto sono:

1. $G^0 = \mathbb{Z}/p^s\mathbb{Z} \rtimes \mathbb{Z}/p^r\mathbb{Z}^*$
2. $G^1 = \mathbb{Z}/p^s\mathbb{Z} \rtimes (\mathbb{Z}/p^r\mathbb{Z}^*)^1$
3. $G^{i+1/(p-1)} = \mathbb{Z}/p^{s-i+1}\mathbb{Z} \rtimes (\mathbb{Z}/p^r\mathbb{Z}^*)^{i+1}$
4. $G^{i+1} = \mathbb{Z}/p^{s-i}\mathbb{Z} \rtimes (\mathbb{Z}/p^r\mathbb{Z}^*)^{i+1}$
5. $G^{s+j+1} = (\mathbb{Z}/p^r\mathbb{Z}^*)^{s+j+1}$

con $1 \leq i \leq s$ e $1 \leq j \leq r - 2 - s$ (con la convenzione che se $r - 2 \leq s$ i gruppi di ramificazione del punto 5. non ci sono).
Anche in questo caso si vede quindi che i salti in alto della ramificazione non sono tutti interi.

Includiamo infine un risultato interessante, cioè il caso in cui $s = r$:
i gruppi di ramificazione con indici in alto di $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^r]{a})/\mathbb{Q}_p$ sono:

1. $G^0 = \mathbb{Z}/p^r\mathbb{Z} \rtimes \mathbb{Z}/p^r\mathbb{Z}^*$
2. $G^1 = \mathbb{Z}/p^r\mathbb{Z} \rtimes (\mathbb{Z}/p^r\mathbb{Z}^*)^1$
3. $G^{i+1/(p-1)} = \mathbb{Z}/p^{r-i+1}\mathbb{Z} \rtimes (\mathbb{Z}/p^r\mathbb{Z}^*)^{i+1}$
4. $G^{i+1} = \mathbb{Z}/p^{r-i}\mathbb{Z} \rtimes (\mathbb{Z}/p^r\mathbb{Z}^*)^{i+1}$
5. $G^{r-1+1/(p-1)} = \mathbb{Z}/p^2\mathbb{Z}$
6. $G^{r+1/(p-1)} = \mathbb{Z}/p\mathbb{Z}$

con $1 \leq i \leq r - 2$.

Osservazione 2.38. E' interessante notare che la proprietà di Hasse-Arf (cioè che i salti in alto della ramificazione di un'estensione abeliana siano interi) caratterizza le p-estensioni abeliane di un campo locale.
Più precisamente, Fesenko ha dimostrato che una p-estensione totalmente ramificata L/K è abeliana se e solo se per ogni estensione abeliana totalmente ramificata E/K l'estensione composta EL/K soddisfa la proprietà di Hasse-Arf. (per ulteriori dettagli si può consultare [Fes]).

Capitolo 3

Class field Theory

In questo capitolo vogliamo trattare i risultati principali sulla teoria delle estensioni abeliane di un campo locale (cioè di un campo completo rispetto ad una valutazione discreta v_K e campo dei residui perfetto). Per i risultati che useremo in seguito possiamo restringerci al caso di campi completi con caratteristica 0 e campo residuo $\overline{K}$ finito.

Le definizioni seguenti e le proprietà di cui non riportiamo le dimostrazioni possono essere ritrovate su [FeV]. Per ulteriori riferimenti sulla teoria della class field, trattata con altri strumenti quali la coomologia di gruppi, si possono consultare [Ser] o [Neu].

3.1 La mappa di Neukirch

Sia K un campo completo rispetto ad una valutazione v_K; supponiamo $charK = 0$, $char\overline{K} = p$ e supponiamo che il campo dei residui $\overline{K}$ sia finito; abbiamo quindi $\overline{K} = \mathbb{F}_q$ con $q = p^f$ e f grado di inerzia dell'estensione. Indichiamo con μ_n il gruppo delle radici n-esime dell'unità.

Vale allora la seguente proposizione:

Proposizione 3.1. *$\forall n \geq 1$ esiste un'unica estensione non ramificata L di K di grado n ed è data da $L = K(\mu_{q^n-1})$; tale estensione L/K è ciclica.*
Se denotiamo con K^{ur} il composto dei tutte le estensioni non ramificate di K allora K^{ur} è la massima estensione non ramificata di K; inoltre è un'estensione di Galois, $Gal(K^{ur}/K) = \hat{\mathbb{Z}}$ ed è topologicamente generato da un automorfismo φ_K tale che:

$$\varphi_K(\alpha) = \alpha^q \pmod{\mathcal{M}_{K^{ur}}} \qquad se\ \alpha \in \mathcal{O}_{K^{ur}}$$

(dove con $\mathcal{M}_{K^{ur}}$ indichiamo come al solito l'unico ideale massimale di $\mathcal{O}_{K^{ur}}$).

Definizione 3.1. L'automorfismo φ_K della proposizione precedente è detto automorfismo di Frobenius.

Sia L/K un'estensione finita e di Galois; si può facilmente notare che la massima estensione non ramificata di L è data da $L^{ur} = LK^{ur}$. Definiamo allora:

$Frob(L/K) = \{ \tilde{\sigma} \in Gal(L^{ur}/K) \mid \tilde{\sigma}_{|_{K^{ur}}}$ è una potenza intera positiva di $\varphi_K \}$.

Definiamo ora il seguente omomorfismo:

Definizione 3.2. Sia L/K un'estensione di Galois. Definiamo la mappa di Neukirch nel modo seguente:

$$\tilde{\Upsilon}_{L/K} : Frob(L/K) \longrightarrow K^*/N_{L/K}(L^*)$$

$$\tilde{\sigma} \longmapsto N_{\Sigma/K}(\pi_\Sigma) \pmod{N_{L/K}(L^*)}$$

dove Σ è il campo fissato da $\tilde{\sigma} \in Frob(L/K)$ e π_Σ è un uniformizzante di Σ.

Si può facilmente dimostrare che la mappa $\tilde{\Upsilon}_{L/K}$ è ben definita (cioè non dipende dagli uniformizzanti scelti).

Supponiamo ora che L/K sia un'estensione finita di Galois e totalmente ramificata; denotiamo con $\mathcal{K} = K^{ur}$ e con $\mathcal{L} = L^{ur}$ le massime estensioni non ramificate rispettivamente di K e di L; allora $Gal(\mathcal{L}/\mathcal{K}) \cong Gal(L/K)$ (in quanto $\mathcal{L} = L\mathcal{K}$ per quanto visto prima e $L \cap \mathcal{K} = K$ perché l'estensione $L \cap \mathcal{K}/K$ è sia non ramificata che totalmente ramificata, quindi è banale).

Definizione 3.3. Per un'estensione $\mathcal{L}/\mathcal{K}$ finita e di Galois denotiamo con $U(\mathcal{L}/\mathcal{K})$ il sottogruppo di $U^1_{\mathcal{L}}$ definito da:

$$U(\mathcal{L}/\mathcal{K}) =< \ u^{\sigma-1} \mid u \in U^1_{\mathcal{L}} \text{ e } \sigma \in Gal(\mathcal{L}/\mathcal{K}) \ > .$$

Vale allora la seguente proposizione:

Proposizione 3.2. *Se π è un uniformizzante di $\mathcal{L}$ definiamo:*

$$l : Gal(\mathcal{L}/\mathcal{K}) \longrightarrow U_{\mathcal{L}}/U(\mathcal{L}/\mathcal{K})$$

$$\sigma \longmapsto \pi^{\sigma-1} \quad (mod\ U(\mathcal{L}/\mathcal{K}))$$

La mappa l è un omomorfismo che non dipende dalla scelta di π. Se indichiamo con $Gal(\mathcal{L}/\mathcal{K})^{ab}$ il massimo quoziente abeliano di $Gal(\mathcal{L}/\mathcal{K})$ allora l induce per passaggio al quoziente un omomorfismo

$$l : Gal(\mathcal{L}/\mathcal{K})^{ab} \longrightarrow U_{\mathcal{L}}/U(\mathcal{L}/\mathcal{K})$$

che rende esatta le seguente successione:

$$1 \longrightarrow Gal(\mathcal{L}/\mathcal{K})^{ab} \xrightarrow{l} U_{\mathcal{L}}/U(\mathcal{L}/\mathcal{K}) \xrightarrow{N_{\mathcal{L}/\mathcal{K}}} U_{\mathcal{K}} \longrightarrow 1 \, .$$

3.2 L'omomorfismo di Hazewinkel

Denotiamo con φ l'estensione continua ad $\mathcal{L}$ dell'automorfismo di Frobenius φ_L e fissiamo un uniformizzante π_L di L. Denotiamo inoltre con E la massima sottoestensione abeliana di L/K.
Si può notare che la norma $N_{\mathcal{L}/\mathcal{K}} : \mathcal{L}^* \to \mathcal{K}^*$ è surgettiva; si può dimostrare infatti che i campi residui di $\mathcal{K}$ e di $\mathcal{L}$ sono algebricamente chiusi, e applicando il corollario 2.24 si ha che $NU_{\mathcal{L}} = U_{\mathcal{K}}$, da cui anche $N\mathcal{L}^* = \mathcal{K}^*$ perchè l'estensione $\mathcal{L}/\mathcal{K}$ è totalmente ramificata.
Per la surgettività della norma si ha quindi che $\forall \alpha \in K^*$ esiste $\beta \in \mathcal{L}^*$ tale che $N_{\mathcal{L}/\mathcal{K}}(\beta) = \alpha$, da cui $N_{\mathcal{L}/\mathcal{K}}(\beta^{\varphi-1}) = \alpha^{\varphi-1} = 1$. Usando la successione esatta della proposizione precedente si ha che, poichè $\beta^{\varphi-1} \in ker(N_{\mathcal{L}/\mathcal{K}})$, esiste $\sigma \in Gal(\mathcal{L}/\mathcal{K})$ tale che

$$\beta^{\varphi-1} \equiv \pi^{1-\sigma} \pmod{U(\mathcal{L}/\mathcal{K})}.$$

Inoltre $\sigma \in Gal(\mathcal{L}/\mathcal{K})^{ab}$, quindi è univocamente determinato come elemento di $Gal(\mathcal{E}/\mathcal{K})$ dove $\mathcal{E} = E\mathcal{K}$.

Definizione 3.4. Definiamo allora l'omomorfismo di Hazewinkel come:

$$\begin{aligned} \Psi_{L/K} : K^*/NL^* &\longrightarrow Gal(L/K)^{ab} \\ \alpha &\longmapsto \sigma_{|_E} \end{aligned}$$

Enunciamo allora il seguente teorema che mostra il legame tra le due mappe precedentemente definite:

Teorema 3.3. *Sia L/K un'estensione di Galois finita totalmente ramificata e sia E/K la massima sottoestensione abeliana di L/K. Allora:*

1. *$\forall \tilde{\sigma} \in Frob(L/K)$ si ha:*

$$\Psi_{L/K}(\tilde{\Upsilon}_{L/K}(\tilde{\sigma})) = \tilde{\sigma}_{|_E};$$

2. *Siano $\alpha \in K^*$ e $\tilde{\sigma} \in Frob(L/K)$ tali che $\tilde{\sigma}_{|_E} = \Psi_{L/K}(\alpha)$; allora:*

$$\tilde{\Upsilon}_{L/K}(\tilde{\sigma}) \equiv \alpha \pmod{N_{L/K}(L^*)}.$$

Di conseguenza $\Psi_{L/K}$ è un isomorfismo, $\tilde{\Upsilon}_{L/K}(\tilde{\sigma})$ non dipende dalla scelta di $\tilde{\sigma}$ per $\sigma \in Gal(L/K)$ e induce l'omomorfismo di Neukirch:

$$\Upsilon_{L/K} : Gal(L/K) \to K^*/N_{L/K}(L^*).$$

Tale mappa induce anche un isomorfismo

$$\Upsilon^{ab}{}_{L/K} : Gal(L/K)^{ab} \longrightarrow K^*/N_{L/K}(L^*)$$

(con $Gal(L/K)^{ab} = Gal(E/K)$) che è esattamente l'inverso di $\Psi_{L/K}$.

Il teorema precedente è stato enunciato per un'estensione totalmente ramificata; in realtà con opportune modifiche la mappa $\Psi_{L/K}$ può essere definita anche per un'estensione L/K di Galois finita (non nec. totalmente ramificata), e l'enunciato del teorema vale ugualmente.

Da tale teorema discende facilmente il corollario seguente (che useremo largamente in seguito):

Corollario 3.4.

- *Sia L/K un'estensione di Galois finita e sia E/K la massima sottoestensione abeliana di L/K; allora $N_{L/K}(L^*) = N_{E/K}(E^*)$.*
- *Sia L/K un'estensione abeliana finita e M/K una sottoestensione di L/K. Allora:*

$$\alpha \in N_{L/M}(L^*) \quad \Longleftrightarrow \quad N_{M/K}(\alpha) \in N_{L/K}(L^*).$$

In seguito daremo una dimostrazione differente di alcuni di questi risultati nel caso specifico di estensioni L/K cicliche.

3.3 Mappa di reciprocità

Definizione 3.5. L'omomorfismo ${\Upsilon^{ab}}_{L/K}$ definito nel teorema 3.3 è un isomorfimo; di conseguenza la mappa inversa definisce un omomorfismo surgettivo:

$$(\ . \ , L/K) : K^* \longrightarrow Gal(L/K)^{ab};$$

Nel caso di estensioni totalmente ramificate $(\ . \ , L/K)$ coincide con l'omomorfismo indotto da $\Psi_{L/K}$.

Denotiamo con K^{ab} la massima estensione abeliana di K; vale allora la seguente proposizione (sui gruppi normici):

Proposizione 3.5.

- *Sia H un sottogruppo di $Gal(L/K)^{ab}$ e sia M il campo fissato da H in $L \cap K^{ab}$; allora $(\ . \ , L/K)^{-1} = N_{M/K}(M^*)$.*
- *Siano L_1 ed L_2 estensioni abeliane di grado finito su K e consideriamo $L_3 = L_1L_2$ e $L_4 = L_1 \cap L_2$. Valgono allora le seguenti relazioni sulle norme:*
  - $N_{L_3/K}(L_3^*) = N_{L_1/K}(L_1^*) \cap N_{L_2/K}(L_2^*)$;
  - $N_{L_4/K}(L_4^*) = N_{L_1/K}(L_1^*)N_{L_2/K}(L_2^*)$.

  Inoltre $L_1 \subset L_2$ se e solo se $N_{L_2/K}(L_2^*) \subset N_{L_1/K}(L_1^*)$; in particolare, si ha l'uguaglianza tra i campi se e solo se anche i gruppi normici associati sono uguali.
- *Se un sottogruppo N in K^* contiene un sottogruppo normico $N_{L/K}(L^*)$ per qualche estensione di Galois finita L/K, allora anche N è un sottogruppo normico (cioè della forma $N_{M/K}(M^*)$ per qualche estensione M/K).*

Grazie alla proposizione precedente possiamo passare al limite proiettivo e definire quindi la "mappa di reciprocità" nel modo seguente:

$$\Psi_K : K^* \longrightarrow \varprojlim K^*/N_{L/K}(L^*) \longrightarrow \varprojlim Gal(L/K)^{ab} = Gal(L^{ab}/K),$$

dove L varia tra tutte le estensioni di Galois finite di K.

Per la mappa Ψ_K valgono le proprietà seguenti:

Teorema 3.6.

- *Ψ_K è ben definita;*
- *l'immagine di Ψ_K è densa in $Gal(K^{ab}/K)$ e il nucleo coincide con l'intersezione di tutti i sottogruppi della forma $N_{L/K}(L^*)$ con L/K estensione di Galois finita;*
- *se L/K è un'estensione di Galois finita e $\alpha \in K^*$ allora l'automorfismo $\Psi_K(\alpha)$ agisce banalmente su $L \cap K^{ab}$ se e solo se $\alpha \in N_{L/K}(L^*)$.*

3.4 Il simbolo di Hilbert

Grazie alle definizioni precedenti siamo pronti a dare la definizione del pairing di Hilbert.
Sia K un campo completo rispetto ad una qualche valutazione discreta v_K; supponiamo che $charK = 0$ e $char\overline{K} = p$. Anche in questo paragrafo ci mettiamo nell'ipotesi in cui il campo residuo $\overline{K}$ sia finito.
Come nella prima sezione indichiamo con μ_n il gruppo delle radici n-esime dell'unità.

Definizione 3.6. Il simbolo di Hilbert $(\ ,\ )_n : K^* \times K^* \longrightarrow \mu_n$ è definito dalla seguente formula:

$$(\alpha, \beta)_n = \gamma^{-1}\Psi_K(\alpha)(\gamma), \quad \text{con } \gamma^n = \beta.$$

Osservazione 3.7. Se δ è un altro elemento con $\delta^n = \beta$, allora $\gamma^{-1}\delta \in \mu_n$ e

$$\delta^{-1}\Psi_K(\alpha)(\delta) = \gamma^{-1}\Psi_K(\alpha)(\gamma),$$

quindi il simbolo di Hilbert è ben definito.

Per il simbolo di Hilbert valgono le seguenti proprietà:

Proposizione 3.8.

1. *$(\ ,\ )_n$ è un'applicazione bilineare;*
2. *$(1-\alpha, \alpha)_n = 1$ per $\alpha \in K^*$ e $\alpha \neq 1$;*
3. *$(-\alpha, \alpha)_n = 1$ per $\alpha \in K^*$;*

4. $(\alpha,\beta)_n = (\beta,\alpha)_n^{-1}$;
5. $(\alpha,\beta)_n = 1$ *se e solo se* $\alpha \in N_{K(\sqrt[n]{\beta})/K}(K(\sqrt[n]{\beta})^*)$ *o equivalentemente se e solo se* $\beta \in N_{K(\sqrt[n]{\alpha})/K}(K(\sqrt[n]{\alpha})^*)$;
6. $(\alpha,\beta)_n = 1$ $\forall \beta \in K^*$ *se e solo se* $\alpha \in K^{*n}$;
7. $(\alpha,\beta)_n = 1$ $\forall \alpha \in K^*$ *se e solo se* $\beta \in K^{*n}$;
8. *se* $\mu_{mn} \subset K^*$ *allora* $(\alpha,\beta)_{nm}{}^m = (\alpha,\beta)_n$ $\forall m \geq 1$;
9. $(\alpha,\beta)_{n,L} = (N_{L/K}(\alpha),\beta)_{n,K}$ *se* $\alpha \in L^*$, $\beta \in K^*$, *dove* $(\ ,\ )_{n,L}$ *e* $(\ ,\ )_{n,K}$ *sono i simboli di Hilbert rispettivamente di* L *e di* K *e* L/K *è un'estensione finita;*
10. $(\sigma\alpha,\sigma\beta)_{n,\sigma L} = \sigma(\alpha,\beta)_{n,L}$, *con* L *èstensione finita di* K, $\sigma \in Gal(K'/K)$, K' *chiusura algebrica di* K *e* $\mu_n \subset L^*$ *ma non necessariamente* $\mu_n \subset K^*$.

Da tali proprietà discende facilmente il seguente il seguente corollario:

Corollario 3.9. *Il simbolo di Hilbert induce il pairing non degenere:*

$$(\ ,\ )_n : K^*/K^{*n} \times K^*/K^{*n} \longrightarrow \mu_n.$$

Fissiamo un campo K e supponiamo che $\mu_n \subset K^*$; utilizzando la teoria di Kummer sappiamo che le estensioni abeliane L/K di esponente n sono in corrispondenza biunivoca con i sottogruppi $B_L \subset K^*$ tali che $B_L \supset K^{*n}$, $L = K(\sqrt[n]{B_L}) = K(\gamma_i :\ \gamma_i^n \in B_L)$ e il gruppo B_L/K^{*n} è duale a $Gal(L/K)$. Con quanto visto finora possiamo dimostrare un'altra corrispondenza; vale infatti il seguente teorema:

Teorema 3.10. *Supponiamo che* $\mu_n \subset K$ *e sia* A *un sottogruppo di* K^* *tale che* $(K^*)^n \subset A$. *Denotiamo con* $B = A^\perp$ *il suo ortogonale rispetto al simbolo di Hilbert* $(\ ,\ )_n$, *cioè:*

$$B = A^\perp = \{\beta \in K^* \mid (\alpha,\beta)_n = 1 \quad \forall \alpha \in A\}.$$

Allora $A = N_{L/K}(L^*)$, *dove* $L = K(\sqrt[n]{B})$ *e* $A = B^\perp$.

Per dimostrare ciò abbiamo bisogno del seguente lemma:

Lemma 3.11. *Sia* K *un campo completo rispetto ad una valutazione discreta con* $charK = 0$ *e supponiamo che* $|\overline{K}| < \infty$. *Allora* K^{*n} *è un sottogruppo di* K^* *di indice finito.*

Dimostrazione. Dimostriamo che $|K/K^{*n}| < \infty$.
Supponiamo che $[K : \mathbb{Q}_p] = m$ e che $\zeta_{p^s} \in K$ con $\zeta_{p^{s+1}} \notin K$. Per il corollario 1.10 si ha che

$$U_K^1 \cong \mathbb{Z}_p^m \times \mathbb{Z}/p^s\mathbb{Z}.$$

(cioè U_K^1 è prodotto di uno $\mathbb{Z}_p$-modulo libero di rango uguale al grado dell'estensione e di una parte di torsione di grado p^s).
Inoltre sappiamo che, se indichiamo con π un uniformizzante di K, si ha:

$$K^* \cong \{\pi^h\}_{h\in\mathbb{Z}} \times U_K \cong \{\pi^h\}_{h\in\mathbb{Z}} \times \overline{K}^{\,*} \times U^1 \cong \{\pi^h\}_{h\in\mathbb{Z}} \times \overline{K}^{\,*} \times \mathbb{Z}_p^m \times \mathbb{Z}/p^s\mathbb{Z}.$$

Calcoliamo K^{*n}:

$$K^{*n} \cong \{\pi^{nh}\}_{h\in\mathbb{Z}} \times (\overline{K}^{\,*})^n \times n\mathbb{Z}_p^m \times n\mathbb{Z}/p^s\mathbb{Z}.$$

Dunque:

$$K^*/K^{*n} \cong \mathbb{Z}/n\mathbb{Z} \times \overline{K}^{\,*}/(\overline{K}^{\,*})^n \times \mathbb{Z}_p^m/n\mathbb{Z}_p^m \times (\mathbb{Z}/p^s\mathbb{Z})/n\mathbb{Z}/p^s\mathbb{Z}.$$

Osserviamo inoltre che, se $n = p^l h$ con $(h, p) = 1$, allora $\mathbb{Z}_p^m/n\mathbb{Z}_p^m \cong \mathbb{Z}/p^l\mathbb{Z}$; di conseguenza:

$$K^*/K^{*n} \cong \mathbb{Z}/n\mathbb{Z} \times \overline{K}^{\,*}/(\overline{K}^{\,*})^n \times \mathbb{Z}/p^l\mathbb{Z} \times (\mathbb{Z}/p^s\mathbb{Z})/n\mathbb{Z}/p^s\mathbb{Z}.$$

Quindi $|K^*/K^{*n}| < \infty$ perché prodotto di gruppi di cardinalità finita.

□

Possiamo ora dimostrare il teorema:

Dimostrazione.
Sia B un sottogruppo di K^* con $K^{*n} \subset B$ e $[B : K^{*n}] = m$. Indichiamo con $A = B^\perp$; allora se, $\alpha \in A$, $\Psi_K(\alpha)$ agisce banalmente su $K(\sqrt[n]{\beta})$ per $\beta \in B$. Infatti, dalla definizione del simbolo di Hilbert abbiamo che

$$(\alpha, \beta)_n = 1 \quad \Longleftrightarrow \quad \gamma^{-1}\Psi_K(\alpha)(\gamma) = 1 \ \text{ con } \gamma^n = \beta.$$

Ciò significa esattamente che $\Psi_K(\alpha)$ agisce banalmente su $L = K(\sqrt[n]{B})$ e, dal teorema 3.6, $\alpha \in N_{L/K}(L^*)$; otteniamo quindi che $A \subset N_{L/K}(L^*)$.
Viceversa, se $\alpha \in N_{L/K}(L^*)$ allora $\Psi_K(\alpha)$ agisce banalmente su $K(\sqrt[n]{\beta}) \subset L$ e

$$\alpha \in N_{K(\sqrt[n]{\beta})/K}(K(\sqrt[n]{\beta})^*)$$

$\forall \beta \in B$. La proprietà (5) della proposizione 3.8 ci dice allora che $(\alpha, \beta)_n = 1$, e quindi che $N_{L/K}(L^*) \subset A$.
Abbiamo quindi dimostrato che $A = N_{L/K}(L^*)$.

Per completare la dimostrazione è sufficiente provare che un sottogruppo A in K^* con $K^{*n} \subset A$ coincide con $(A^\perp)^\perp$.
Per fare ciò notiamo che, la restrizione del simbolo di Hilbert a $A \times K^*$ induce un pairing non degenere

$$(\ ,\ )_n : A/K^{*n} \times K^*/A^\perp \longrightarrow \mu_n.$$

Vale allora il seguente risultato più generale (che discende da proprietà dei gruppi abeliani finiti):

Teorema 3.12. *Sia $A \times A' \to C$ una mappa bilineare dal prodotto di due gruppi abeliani A e A' in un gruppo ciclico C di ordine m. Siano B e B' i rispettivi nuclei sinistro e destro dell'applicazione, e supponiamo che A'/B' sia finito. Allora A/B è finito e A'/B' è isomorfo al duale del gruppo A/B.*

(per una dimostrazione di tale risultato si può consultare [La2], teorema 9.2 pp. 49).

Nel nostro caso il pairing è non degenere; di conseguenza $B = B' = \{1\}$, da cui A/K^{*n} è isomorfo al duale di $K^*/A^\perp$. Essendo i gruppi finiti ciò implica che

$$|A/K^{*n}| = |K^*/A^\perp|.$$

Con le stesse tecniche possiamo dimostrare che l'ordine di $K^*/A^\perp$ è uguale all'ordine di $(A^\perp)^\perp/K^{*n}$ da cui otteniamo quindi

$$|A/K^{*n}| = |(A^\perp)^\perp/K^{*n}|.$$

Notiamo inoltre che banalmente $A \subset (A^\perp)^\perp$; infatti, se $\alpha \in A$, allora $(\alpha, \beta)_n = 1\ \forall \beta \in A^\perp$, da cui $\alpha \in (A^\perp)^\perp$; per l'uguaglianza degli ordini si ha dunque $A = (A^\perp)^\perp$.

□

Osservazione 3.13. Notiamo che, se $charK = 0$, presa L/K è un'estensione di Galois finita di grado n allora $N_{L/K}(L^*)$ è di indice finito in K^*.
Infatti banalmente $K^{*n} \subset N_{L/K}(L^*)$ e dal lemma 3.11 sappiamo che K^{*n} è di indice finito in K^*; di conseguenza anche $N_{L/K}(L^*)$ è di indice finito in K^*.

Vogliamo ora generalizzare il teorema precedente al caso generale in cui il campo K non contenga necessariamente le radici n-esime dell'unità.

Vale allora il seguente teorema generale:

Teorema 3.14 (Teorema di esistenza)**.** *Sia K un campo completo rispetto ad una valutazione discreta; supponiamo che $charK = 0$ e che $|\overline{K}| < \infty$. Esiste allora una corrispondenza biunivoca tra le estensioni abeliane finite di K e i sottogruppi di indice finito di K^* data da:*

$$L/K \longleftrightarrow N_{L/K}(L^*).$$

Tale corrispondenza è una bigezione che inverte l'ordine tra il reticolo dei sottoruppi aperti di indice finito di K^* (rispetto ad intersezione $N_1 \cap N_2$ e prodotto N_1N_2) e il reticolo delle estensioni abeliane finite di K^* (rispetto ad intersezione $L_1 \cap L_2$ e composto L_1L_2).

Dimostrazione. Abbiamo precedentemente visto che se L/K è un'estensione abeliana finita allora $N_{L/K}(L^*)$ è un sottogruppo di K^* di indice finito. Verifichiamo allora che un sottogruppo N di indice finito in K^* coincide con il sottogruppo $N_{L/K}(L^*)$ per qualche estensione abeliana finita L di K. Per fare ciò è sufficiente dimostrare che N contiene il sottogruppo normico $N_{L/K}(L^*)$ per qualche estensione finita L di K. Se vale ciò infatti, indicando con $\tilde{L}$ la chiusura normale di L su K, si ha:

$$N_{\tilde{L}/K}(\tilde{L}^*) = N_{L/K}(N_{\tilde{L}/L}(\tilde{L}^*)) \subset N_{L/K}(L^*) \subset N.$$

Di conseguenza N contiene il sottogruppo normico di un'estensione di Galois finita $\tilde{L}/K$, e per la proposizione 3.5 deduciamo che $N = N_{M/K}(M^*)$ dove M è il campo fissato da $(N, \tilde{L}/K)$ e M/K è un'estensione abeliana.

Denotiamo allora con n l'indice di N in K^* e distinguiamo due casi:

- Supponiamo che $\mu_n \subset K^*$; allora applicando il teorema 3.10 si ha che ${K^*}^n = N_{L/K}(L^*)$ per una qualche estensione abeliana finita L/K, in quanto ${K^*}^n$ è di indice finito in K^*; di conseguenza $N_{L/K}(L^*) \subset N$.

- Supponiamo che $\mu_n \not\subset K^*$ e indichiamo con $K_1 = K(\mu_n)$; allora K_1 è un'estensione finita di K. Applicando il teorema 3.10 al campo K_1 si ha che $K_1^{*n} = N_{L/K_1}(L^*)$ con L/K_1 estensione abeliana finita; di conseguenza abbiamo

  $$N_{L/K}(L^*) = N_{K_1/K}(N_{L/K_1}(L^*)) = N_{K_1/K}(K_1^{*n}) \subset {K^*}^n \subset N,$$

  da cui la tesi. (osserviamo che in questo caso l'estensione L/K è finita ma non necessariamente abeliana; tuttavia per l'osservazione fatta all'inizio della dimostrazione questo basta per ottenere il teorema).

□

Definizione 3.7. Il campo L tale che L/K è un'estensione abeliana di grado finito con la proprietà per cui $N_{L/K}(L^*) = N$ è detto "class field" del sottogruppo $N \subset K^*$.

Osservazione 3.15. Per completezza osserviamo che il teorema di esistenza può essere enunciato in modo analogo anche se il campo K ha caratteristica $p \neq 0$, a patto di prendere i sottogruppi N di K^* aperti e di indice finito; in questo caso dunque vale:

Teorema 3.16. *Esiste allora una corrispondenza biunivoca tra le estensioni abeliane finite di K e i sottogruppi aperti di K^* di indice finito data da:*

$$N \longleftrightarrow N_{L/K}(L^*).$$

Tale corrispondenza è una bigezione che inverte l'ordine tra il reticolo dei sottoruppi aperti di indice finito di K^* (rispetto ad intersezione $N_1 \cap N_2$ e prodotto N_1N_2) e il reticolo delle estensioni abeliane finite di K^* (rispetto ad intersezione $L_1 \cap L_2$ e composto L_1L_2).

Tale enunciato è coerente con il caso particolare trattato prima. Infatti, se $charK = 0$, ogni sottogruppo N di K^* di indice finito è aperto. Ciò discende dalla seguente proposizione:

Proposizione 3.17. *Sia K un campo completo rispetto ad una certa valutazione discreta. Se $charK = 0$ e $char\overline{K} = p$ allora K^{*n} è un sottogruppo aperto di K^* $\forall n \geq 1$.*

Dimostrazione. Supponiamo che $char\overline{K} = p$ e distinguiamo due casi:

- supponiamo $(n, p) = 1$. Allora $U_1 \subset K^{*n}$ e dunque K^{*n} è aperto;
- supponiamo $n = p^m$ per qualche $m \geq 1$. Osserviamo che, se $charK = 0$, vale che $U_i \subset U_{i-e}^p$ se $i > \dfrac{pe}{p-1}$. Iterando quindi si ha che, $U_{i-e} \subset U_{i-2e}^p$ se $i - e > \dfrac{pe}{p-1}$, da cui $U_i \subset U_{i-e}^p \subset U_{i-2e}^{p^2}$.
  Iterando ancora si ha

  $$\text{se } i > \frac{pe}{p-1} + (m-1)e \quad U_i \subset U_{i-me}^{p^m} \subset K^{*p^m}.$$

  Di conseguenza K^{*p^m} è aperto.

I due casi combinati insieme mostrano che il lemma vale $\forall n \geq 1$.

□

3.5 Due dimostrazioni per via elementare

Diamo ora una dimostrazione più diretta di due proprietà fondamentali sui gruppi normici senza fare uso della teoria della class field.

Sia K un campo completo rispetto ad una valutazione discreta v_K con $charK = 0$ e supponiamo che il campo dei residui $\overline{K}$ sia finito. Indichiamo con $p = char\overline{K}$; vale allora la seguente proposizione:

Proposizione 3.18. *Sia L/K un'estensione ciclica di grado l, con l primo; allora $K^*/N_{L/K}(L^*)$ è un gruppo ciclico di ordine l.*

Dimostrazione. Distinguiamo vari casi:

- Supponiamo che l'estensione L/K sia non ramificata;
  dal corollario 2.5 del capitolo 2 abbiamo che la proprietà $\overline{K} = N_{L/K}(\overline{L})$ (che qui è verificata perchè i campi residui sono finiti) è equivalente al fatto che l'indice di $N_{L/K}(L^*)$ in K^* sia esattamente il grado di inerzia f, dunque in questo caso $|K^*/N_{L/K}(L^*)| = l$. Essendo l primo si ha quindi che $K^*/N_{L/K}(L^*)$ è ciclico di ordine l.

- Supponiamo che l'estensione L/K sia totalmente ramificata; distinguiamo due ulteriori sottocasi:

  - Supponiamo $(l, p) = 1$; l'estensione è dunque di tipo tame.
    Poiché L/K è totalmente ramificata, esiste un uniformizzante π di K tale che $\pi \in N_{L/K}(L^*)$, quindi $K^*/N_{L/K}(L^*) \cong U_K/N_{L/K}(U_L)$ (come visto nel corollario 2.19). Notiamo che nel caso di estensioni totalmente ramificate tame di grado primo allora l'unico salto della ramificazione si ha per $t = 0$; di conseguenza, applicando il corollario 2.16, si ha che $N_{L/K}(U_L^1) = U_K^1$. Sia ora $\theta \in U_K$; allora possiamo scrivere $\theta = \overline{\theta}u$ con $\overline{\theta} \in \overline{K} = \mathbb{F}_q$ e $u \in U_K^1$. D'altra parte esiste $v \in U_L^1$ tale che $u = N_{L/K}(v)$; di conseguenza $\theta = \overline{\theta}N_{L/K}(v)$. Abbiamo dunque che $\theta \in N_{L/K}(U_L)$ se e solo se $\overline{\theta} \in N(\mathbb{F}_q) = \mathbb{F}_q^l$ in quanto l'estensione è totalmente ramificata. Possiamo quindi scrivere
    $$N_{L/K}(L^*) =< \pi > \times \mathbb{F}_q^{*l} \times U_K^1;$$
    inoltre sappiamo che in generale
    $$K^* =< \pi > \times \mathbb{F}_q^* \times U_K^1,$$

quindi quozientando otteniamo:

$$K^*/N_{L/K}(L^*) \cong \mathbb{F}_q^*/\mathbb{F}_q^{*l}.$$

Ora, essendo l'estensione L/K di Galois, $\mu_l \subset K^*$ (dove con μ_l indichiamo il gruppo delle radici l-esime dell'unità) e quindi $l \mid q-1$. Di conseguenza il sottogruppo $\mathbb{F}_q^{*l}$ è un sottogruppo di $\mathbb{F}_q^*$ indice l, e dunque $\mathbb{F}_q^*/\mathbb{F}_q^{*l}$ è ciclico di ordine l. Abbiamo dunque:

$$K^*/N_{L/K}(L^*) \cong \mathbb{F}_q^*/\mathbb{F}_q^{*l} \cong \mathbb{Z}/l\mathbb{Z}.$$

– Supponiamo $l = p$; allora l'estensione è di tipo wild.
Come nel caso precedente, esiste un uniformizzante π di K tale che $\pi \in N_{L/K}(L^*)$, quindi $K^*/N_{L/K}(L^*) \cong U_K/N_{L/K}(U_L)$ (come visto nel corollario 2.19). Inoltre, poiché il campo dei residui $\overline{K}$ è finito, in particolare è perfetto, quindi $\overline{K} = \overline{K}^{\,p}$ e

$$U_K/N_{L/K}(U_L) \cong U_K^1/N_{L/K}(U_L^1).$$

Sia $t > 0$ l'unico salto della ramificazione; applicando il corollario 2.15 si ha

$$U_K^i/U_K^{i+1}N_{L/K}(U_L^i) = \{1\}.$$

Di conseguenza abbiamo che

$$U_K^i = U_K^{i+1}N_{L/K}(U_L^i) \quad \forall 1 \le i < t,$$

da cui

$$U_K^1 = U_K^2 N_{L/K}(U_L^1) = U_K^3 N_{L/K}(U_L^2)N_{L/K}(U_L^1) = \ldots = U_K^s N_{L/K}(U_K^1).$$

Si ha quindi che

$$U_K^1/N_{L/K}(U_L^1) \cong U_K^s N_{L/K}(U_L^1)/N_{L/K}(U_L^1) \cong U_K^s/(U_K^s \cap N_{L/K}(U_L^1)).$$

D'altra parte sappiamo che $U_K^s \supset U_K^s \cap N_{L/K}(U_L^1) \supset N_{L/K}(U_L^s)$ e, poiché per il corollario 2.18 si ha che $U_K^s/N_{L/K}(U_L^s) \cong \overline{K}/\mathcal{P}(\overline{K})$ (che nel caso in cui $\overline{K}$ è finito ha ordine p come già osservato nel capitolo 1) allora $U_K^s \cap N_{L/K}(U_L^1) = N_{L/K}(U_L^s)$. Di conseguenza:

$$K^*/N_{L/K}(L^*)U_K^1/N_{L/K}(U_L^1) \cong U_K^s/N_{L/K}(U_L^s) \cong \mathbb{Z}/p\mathbb{Z}$$

cioè $K^*/N_{L/K}(L^*)$ è un gruppo ciclico di ordine p.

Osservazione 3.19. Poiché $U_K^s \not\subset N_{L/K}(U_L^1)$, si ha che un generatore del gruppo ciclico $K^*/N_{L/K}(L^*)$ può essere preso della forma $(1+\theta\pi_K^s)N_{L/K}(L^*)$.

□

Generalizziamo la proposizione appena dimostrata:

Teorema 3.20. *Sia L/K un'estensione ciclica di grado n, con n qualsiasi; allora $K^*/N_{L/K}(L^*)$ è un gruppo ciclico di ordine n.*

Dimostrazione. Dimostriamo il teorema per induzione sulla lunghezza della fattorizzazione di n:

- Passo base: se n è primo il teorema si riduce alla proposizione precedente;
- Passo induttivo: supponiamo che n non sia primo; sia σ un generatore di $Gal(L/K)$ e sia M/K una sottoestensione non banale di L/K. Definiamo:
$$M^{*\sigma-1} = \{\ \alpha^{-1}\sigma(\alpha) \mid \alpha \in M^*\};$$
vogliamo dimostrare inizialmente le due proprietà seguenti:
$$M^{*\sigma-1} \subset N_{L/M}(L^{*\sigma-1}) \quad \text{e} \quad M^* \subset K^* N_{L/M}(L^*).$$
Dimostriamo che $M^{*\sigma-1} \subset N_{L/M}(L^{*\sigma-1})$. Anche qui facciamo la dimostrazione per induzione sulla lunghezza della fattorizzazione del grado $[L:M]$.
  - Supponiamo che $[L:M]$ sia primo; allora per il punto precedente $M^*/N_{L/M}(L^*)$ è un gruppo ciclico dello stesso grado.
    Indichiamo con $\alpha N_{L/M}(L^*)$ un generatore di $M^*/N_{L/M}(L^*)$.
    Essendo $M^*/N_{L/M}(L^*)$ ciclico, vale che $\alpha^{-1}\sigma(\alpha) \in N_{L/M}(L^*)$; di conseguenza $\exists\ \beta \in L^*$ tale che $\alpha^{-1}\sigma(\alpha) = N_{L/M}(\beta)$. D'altra parte si vede facilmente che
    $$N_{L/K}(\beta) = N_{M/K}(N_{L/M}(\beta)) = N_{M/K}(\alpha^{-1}\sigma(\alpha)) = 1,$$
    in quanto α e $\sigma(\alpha)$ sono coniugati in M/K dunque hanno la stessa norma.
    Usando allora il teorema 90 di Hilbert si vede che $\exists\ \gamma \in L^*$ tale che $\beta = \sigma(\gamma)/\gamma$. Ciò dimostra che $M^{*\sigma-1} \subset N_{L/M}(L^{*\sigma-1})$.

– Supponiamo che $[L : M]$ non sia primo.
Sia allora M_1/M una sottoestensione propria di L/M; per ipotesi induttiva sappiamo che

$$(M^*)^{\sigma-1} \subset N_{M_1/M}(M_1^{*\sigma-1})$$

e

$$(M_1^*)^{\sigma-1} \subset N_{L/M_1}(L^{*\sigma-1}).$$

Per le proprietà di composizione delle norme, si ha dunque:

$$(M^*)^{\sigma-1} \subset N_{M_1/M}(M_1^{*\sigma-1}) \subset N_{M_1/M}(N_{L/M_1}(L^{*\sigma-1})) = N_{L/M}(L^{*\sigma-1}).$$

Ciò dimostra la prima asserzione.

Dimostriamo ora che $M^* \subset K^* N_{L/M}(L^*)$.
Sia $\alpha \in M^*$; poichè $(M^*)^{\sigma-1} \subset N_{L/M}(L^{*\sigma-1})$ esiste $\gamma \in L^*$ tale che:

$$\alpha^{-1}\sigma(\alpha) = N_{L/M}(\gamma^{-1}\sigma(\gamma)) = (N_{L/M}(\gamma))^{-1}\sigma(N_{L/M}(\gamma)).$$

Se chiamiamo $\beta = N_{L/M}(\gamma)$ allora β è un elemento di $N_{L/M}(L^*)$ tale che:

$$\alpha^{-1}\sigma(\alpha) = \beta^{-1}\sigma(\beta).$$

Utilizzando ciò abbiamo che $\sigma(\alpha\beta^{-1}) = \alpha\beta^{-1}$; di conseguenza, essendo $< \sigma >= Gal(L/K)$, si ha $\alpha\beta^{-1} \in Fix(< \sigma >) = K$ e quindi

$$M^* \subset K^* N_{L/M}(L^*).$$

Dimostriamo ora il teorema.
Supponiamo per assurdo che esista un divisore proprio m di n tale che ${K^*}^m \subset N_{L/K}(L^*)$. Sia allora M/K l'unica sottoestensione di L/K di grado m; allora:

$$N_{M/K}(K^*) = (K^*)^m \subset N_{L/K}(L^*)$$

(in quanto se $\beta \in K^*$ allora $N_{M/K}(\beta) = \beta^m$).
Utilizzando tale relazione e il teorema 90 di Hilbert deduciamo che $K^* \subset N_{L/M}(L^*)(M^*)^{\sigma-1}$.
Sia infatti $\beta \in K^*$; allora $N_{M/K}(\beta) = \beta^m \subset N_{L/K}(L^*)$. Di conseguenza esiste $\gamma \in L^*$ tale che

$$N_{M/K}(\beta) = N_{M/K}(N_{L/M}(\gamma)), \quad \text{da cui} \quad N_{M/K}(\beta(N_{L/M}(\gamma))^{-1}) = 1.$$

Possiamo allora applicare il teorema 90 all'elemento $\beta(N_{L/M}(\gamma))^{-1}$; esiste quindi $\alpha \in M^*$ tale che

$$\beta(N_{L/M}(\gamma))^{-1} = \alpha^{-1}\sigma(\alpha) \in M^{*\sigma-1}.$$

Di conseguenza otteniamo $\beta = \alpha^{-1}\sigma(\alpha)(N_{L/M}(\gamma))$, da cui

$$\beta \in (N_{L/M}(L^*))M^{*\sigma-1}.$$

Inoltre, utilizzando le relazioni dimostrate prima, si ha:

$$K^* \subset (N_{L/M}(L^*))M^{*\sigma-1} \subset (N_{L/M}(L^*))N_{L/M}(L^{*\sigma-1}) = N_{L/M}(L^*).$$

D'altra parte, grazie alla relazione $M^* \subset K^*N_{L/M}(L^*)$, si ha:

$$M^* \subset K^*N_{L/M}(L^*) \subset N_{L/M}(L^*) \subset M^*,$$

il che è impossibile perchè $M^* \neq N_{L/M}(L^*)$ (infatti $M^*/N_{L/M}(L^*)$ è un gruppo di ordine maggiore o uguale ad l, dove l è un primo che divide n/m, per quanto visto nella proposizione precedente).
Abbiamo dunque che, $\forall m$ divisore proprio di n, $(K^*)^m \notin N_{L/K}(L^*)$.
D'altra parte:

$$[K^* : N_{L/K}(L^*)] = [K^* : N_{M/K}(M^*)][N_{M/K}(M^*) : N_{M/K}(N_{L/K}(L^*))]$$
$$\leq [K^* : N_{M/K}(M^*)][M^* : N_{L/M}(L^*)].$$

Ma, utilizzando l'ipotesi induttiva, si ha che

$$[K^* : N_{M/K}(M^*)] = [M : K] \text{ e } [M^* : N_{L/M}(L^*)] = [L : M],$$

quindi sostituendo otteniamo:

$$[K^* : N_{L/K}(L^*)] \leq [L : M][M : K] = n.$$

Di conseguenza otteniamo che $K^*/N_{L/K}(L^*)$ è ciclico di ordine n, da cui la tesi.

□

Da tale teorema segue direttamente il corollario seguente:

Corollario 3.21. *Sia L/K un'estensione ciclica di grado l^n, con l primo e $n \geq 1$ e sia M/K la sottoestensione di grado l^{n-1} in L/K. Sia $\alpha \in K^*$; allora:*

$$\alpha^l \in N_{L/K}(L^*) \quad \Longleftrightarrow \quad \alpha \in N_{M/K}(M^*).$$

Dimostrazione. Dimostriamo le due implicazioni:

$\Leftarrow$ Supponiamo $\alpha \in N_{M/K}(M^*)$; allora $\exists \beta \in M^*$ tale che $\alpha = N_{M/K}(\beta)$. Essendo $[L : M] = l$, si ha:

$$\alpha^l = (N_{M/K}(\beta))^l = N_{L/K}(\beta), \quad \text{da cui} \quad \alpha^l \in N_{L/K}(L^*).$$

$\Rightarrow$ Supponiamo $\alpha^l \in N_{L/K}(L^*)$; allora $[\alpha^l] = [\alpha]^l = [0]$ in $K^*/N_{L/K}(L^*)$. D'altra parte la proposizione precedente dice che $K^*/N_{L/K}(L^*)$ è un gruppo ciclico di ordine l^n. Poiché $[\alpha]$ ha ordine l in $K^*/N_{L/K}(L^*)$, $[\overline{\alpha}]$ appartiene all'unico sottogruppo di ordine l di $K^*/N_{L/K}(L^*)$ che è proprio $N_{M/K}(M^*)/N_{L/K}(L^*)$.
Di conseguenza $\alpha \in N_{M/K}(M^*)$.

□

Capitolo 4

Due casi concreti

Prima di trattare il caso generale della caratterizzazione dei salti della ramificazione di un'estensione ciclica di grado p^m vogliamo approfondire quali sono le proprietà del salto di un'estensione ciclica di grado p nel caso in cui il campo K contenga le radici p-esime dell'unità.

Da tale caso seguirà anche la caratterizzazione dei salti di un'estensione L/K con gruppo di Galois $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

4.1 Estensioni cicliche di grado p

Sia K un campo completo rispetto ad una valutazione discreta v_K con *char* $K = 0$ e *char* $\overline{K} = p \neq 0$. Supponiamo inoltre che il campo sia tale che $|\overline{K}| < \infty$ (dunque in particolare il campo dei residui è perfetto) e che K contenga le radici p-esime dell'unità. Poniamo $e' = e_K/(p-1)$ (che è intero in quanto le radici p-esime appartengono al campo).

Sia M/K un'estensione ciclica totalmente ramificata di grado p; allora essa ha un unico salto in alto della ramificazione, che coincide con il salto in basso. Notiamo che, per la teoria di Kummer (che possiamo applicare in quanto siamo nelle ipotesi per cui $\zeta_p \in K$) $M = K(\sqrt[p]{x})$, per qualche $x \in K^*$. Cambiando x a meno di potenze p-esime possiamo supporre che $0 \leq v_K(x) < p$.

Proposizione 4.1. *Se $M = K(\sqrt[p]{x})$ con $0 < v_K(x) < p$ allora M/K è totalmente ramificata con salto di ramificazione $t = pe/(p-1)$.*

Dimostrazione. Indichiamo con z una radice p-esima di x.
Osserviamo innanzitutto che, se $\forall h$ tale che $(h, p) = 1$ si ha $K(z) = K(z^h)$;

possiamo allora ridurci al caso $v_K(x) = 1$. In tal caso $\pi = \zeta$ è un uniformizzante di M e l'estensione M/K è totalmente ramificata. Indichiamo con g un generatore di $Gal(M/K)$ e calcoliamo allora $v_K(g(\pi) - \pi)$:

$$v_M(g(\pi) - \pi) = v_M(\zeta\pi - \pi) = v_M(\zeta - 1) + v_M(\pi) = e'_M + 1 = \frac{pe}{p-1} + 1.$$

Poiché il salto della ramificazione soddisfa la relazione $v_M(g(\pi) - \pi) = t + 1$, si ha

$$t = \frac{pe}{p-1}.$$

□

Consideriamo ora le estensioni della forma $K(\sqrt[p]{x})$ con $v_K(x) = 0$; vogliamo studiarne i salti. Per fare ciò è utile ridurci ad alcuni casi particolari; dimostriamo la seguente proposizione:

Proposizione 4.2. *Sia $x \in U_K$. Allora x è moltiplicativamente congruente modulo K^{*p} ad un'unità y con $v_K(y-1) = s$, dove s ha una delle seguenti proprietà:*

1. *$1 \leq s < pe'$ e $(p, s) = 1$ oppure*
2. *$s = pe'/(p-1)$ oppure*
3. *$s = +\infty$ (cioè $y = 1$).*

Dimostrazione.
Per ipotesi sappiamo che il campo dei residui $\overline{K}$ è finito; in particolare quindi $\overline{K}$ è un campo perfetto. In generale vale che $U_K/U_K^1 \cong \overline{K}^*$ (come visto nella proposizione 1.3 del capitolo 1); di conseguenza a meno di moltiplicare x per una potenza p-esima possiamo supporre che $x \in U_K^1$. Distinguiamo vari casi:

- Supponiamo che $x \in U_K^i$, con $i > pe/(p-1)$; allora poiché $U_K^i = (U_K^{i-e})^p$ siamo nel caso in cui $x \in K^{*p}$, dunque vale la condizione (3);
- Supponiamo ora che $v_K(x-1) = i < pe/(p-1)$ e che $i = pt$ per qualche intero t. Allora dal corollario 1.6 del capitolo 1 esiste $z \in U_K^{pt}$ tale che $xz^p \in U_K^{pt+1}$. Supponiamo che $v_K(xz^p - 1) = i_1 \geq pt + 1$ e distinguiamo due casi:
  - Se $(p, i_1) = 1$ oppure $i_1 = pe/(p-1)$ allora $x \equiv y \ (mod\ K^{*p})$ con $v_K(y-1) = i_1$ e i_1 soddisfa la tesi;

– se ciò non accade, possiamo ripetere il processo e concludere la dimostrazione per induzione.

□

Osservazione 4.3. La proposizione precedente ci dice che, se $L = K(\sqrt[p]{x})$ con $v_K(x) = 0$, possiamo scegliere un opportuno generatore z in modo che $L = K(z)$ con $z^p = u_l$, $v_K(u_l - 1) = l$ e tale che l che soddisfa le condizioni della proposizione precedente. Ci restringiamo dunque a studiare estensioni con generatori di questo tipo.

Valgono allora i seguenti teoremi:

Teorema 4.4. *Sia $M = K(\sqrt[p]{u_l})$; allora*

$$M/K \text{ è un'estensione non ramificata} \iff l = pe/(p-1).$$

Per dimostrare tale teorema ricordiamo l'enunciato del classico Lemma di Hensel. Una dimostrazione di questo risultato può essere trovata su [Neu].

Proposizione 4.5 (Lemma di Hensel)**.** *Siano K un campo completo rispetto ad una valutazione discreta, $\mathcal{O}_K$ l'anello di valutazione e $\mathcal{M}_k$ il rispettivo ideale massimale; sia inoltre $f(x)$ un polinomio a coefficienti in $\mathcal{O}_K$ e indichiamo con $\overline{f}$ la riduzione di f in $\overline{K}$.*
Supponiamo che $\overline{f} = \overline{g}\overline{h}$ con $(\overline{g}, \overline{h}) = 1$; allora esistono $G(x), H(x) \in \mathcal{O}_K[x]$ tali che $deg G = deg\ \overline{g}$, $\overline{G} = \overline{g}$, $\overline{H} = \overline{h}$ e $f = GH$.

Dimostriamo quindi il teorema 4.4:

Dimostrazione.

⇐) Chiamiamo $z = \sqrt[p]{u_l}$ con $l = pe/(p-1)$ e mostriamo che l'estensione $K(z)/K$ è totalmente ramificata. Sia $y = 1/(1-\zeta)$, dove con ζ indichiamo una radice primitiva dell'unità, e scriviamo $w = y(z-1) \in M$. Allora w è un radice di un polinomio irriducibile $f(X) = (X+y)^p - u_l y^p$, e $M = K(y)$. Possiamo scrivere $f(X)$ nella forma:

$$f(X) = X^p + \sum_{i=1}^{p-1} (C_i) y^{p-i} X^i + (1 - u_l) y^p.$$

Notiamo che $f(X)$ è a coefficienti interi. Infatti $p \mid C_i$ $\forall i$ tale che $1 \le i < p$, quindi

$$v_K(C_i y^{p-i}) \ge v_K(C_i) - (p-i) v_K(1\zeta) \ge (p-1)e' - (p-i)e' \ge 0$$

e $v_K(1-u_l) = pv_K(1-\zeta)$, quindi anche $v_K(1-u_l)y^p \geq 0$. Inoltre, $v_K(C_i)y^{p-i} > 0$ per $1 < i < p$, quindi se consideriamo il polinomio ridotto in $\overline{K}$ esso sarà della forma

$$\overline{f}(X) = X^p + \overline{b}X + \overline{a}, \quad dove\ a = (1-x)y^p\ e\ b = py^{p-1}.$$

Si vede allora che $\overline{f}(X)$ ha radici distinte in quanto $\overline{a} \neq 0$, $\overline{b} \neq 0$ e $\overline{f}'(X) = \overline{b}$; inoltre, dato che $\overline{f}(X)$ ha grado p primo, esso o è irriducibile in $\overline{K}[X]$ o ha una radice in $\overline{K}$. Tuttavia, se per assurdo $\overline{f}(X)$ avesse una radice in $\overline{K}$, allora per il lemma di Hensel 4.5 $f(X)$ dovrebbe avere una radice in K, il che è assurdo.
Di conseguenza $\overline{f}(X)$ è irriducibile su $\overline{K}[X]$, $[\overline{M} : \overline{K}] = p$ e M/K è non ramificata.

$\Rightarrow$) Supponiamo che M/K sia non ramificata. Scriviamo $M = K(z)$, dove $x = z^p$ può essere scelto in U_K per la proposizione 4.1. Indichiamo con $i = v_K(x-1)$; come visto precedentemente si ha che, a meno di cambiare x per una potenza p-esima possiamo supporre che

$$1 \leq i \leq pe/(p-1)\ \ e\ \ i \not\equiv 0\ \ (p)\ \ se\ i \neq pe/(p-1).$$

Dato che M/K è non ramificata, vale anche che $v_M(x-1) = v_K(x-1) = i$. Ma il corollario 1.6 del capitolo 1 ci dice che $v_M(x-1) = p\ v_M(z-1)$, dunque $p \mid i$ e di conseguenza si ha che necessariamente $i = pe/(p-1)$.

□

Resta infine da trattare il caso di un'estensione totalmente ramificata con salto della ramificazione $t < pe/(p-1)$. Vale allora il seguente teorema:

Teorema 4.6. *Sia $M = K(\sqrt[p]{u_l})$ con $v_K(u_l - 1) = l$ tale che $1 \leq l < pe'/(p-1)$ con $(l,p) = 1$. Allora M/K è un'estensione totalmente ramificata con salto della ramificazione pari a*

$$t = pe/(p-1) - l.$$

Per dimostrare il teorema appena enunciato ricorriamo al seguente lemma che calcora il valore del discriminante di queste particolari estensioni:

Lemma 4.7. *Sia K un campo completo rispetto ad una valutazione discreta con char $K = 0$ sia $p = char\ \overline{K}$; supponiamo inoltre che $\zeta_p \in K$ (cioè che K contenga le radici p-esime dell'unità); sia inoltre L un'estensione ciclica di K di grado p del tipo $L = K(\sqrt[p]{u_l})$ con $u_l \in U_K^l - U_K^{l+1}$, $1 \leq l < pe_K/(p-1)$ e $(l,p) = 1$. Allora:*

$$disc(L/K) = (\ \pi^{(p-1)(pe_K/(p-1)-l+1)}\ ).$$

Dimostrazione. Indichiamo con λ un generatore di $Gal(L/K)$, π un uniformizzante di K e con γ una radice p-esima di u_l. Osserviamo allora che $\gamma \in U_L^l$.
Infatti sia π_L un uniformizzante di L; allora $\exists\ h$ tale che

$$\gamma = 1 + a\pi_L^h \quad \text{e} \quad v_L(a) = 0;$$

d'altra parte $\gamma^p = (1 + a\pi_L^h)^p$ e quindi $v_L(\gamma^p - 1) = min\{hp,\ h + e\}$.
Ma $\gamma^p = u_l$, quindi

$$v_L(\gamma^p - 1) = min\{hp,\ h + e\} = v_L(u_l - 1) = pv_F(u_l - 1) = pl\ ;$$

di conseguenza $h = l$ e dunque $\gamma \in U_L^l$.

Denotiamo con l' un intero tale che $ll' \equiv 0\ (p)$; allora l'elemento

$$\pi_L = \frac{(\gamma - 1)^{l'}}{\pi^{(ll'-1)/p}}$$

è un uniformizzante di L; infatti:

$$\begin{aligned} &v_L(\gamma - 1)^{l'} = l'v_L(\gamma - 1) = ll';\\ &v_L(\pi^{(ll'-1)/p}) = pv_F(\pi^{(ll'-1)/p}) = ll' - 1 \end{aligned}$$

da cui, sostituendo:

$$v_L(\pi_L) = ll' - (ll' - 1) = 1.$$

Calcoliamo allora il differente dell'estensione:

$$\mathcal{D}_{L/K} = \prod_{i=1}^{p-1}(\lambda^i(\pi_L) - \pi_L).$$

Notiamo che $(ll' - 1)/p \in \mathbb{Z}$, quindi $\pi^{(ll'-1)/p}$ è fissato da $\lambda^i\ \forall i$; sostituendo allora l'espressione di π_L si ha:

$$\begin{aligned} \mathcal{D}_{L/K} &= \frac{1}{\pi^{(p-1)(ll'-1)/p}} \prod_{i=1}^{p-1} (\lambda^i(\gamma - 1)^{l'} - (\gamma - 1)^{l'})\\ &= \frac{1}{\pi^{(p-1)(ll'-1)/p}} \prod_{i=1}^{p-1} ((\zeta_p^i\gamma - 1)^{l'} - (\gamma - 1)^{l'}). \end{aligned}$$

Riscriviamo il prodotto utilizziamo la relazione $a^h - b^h = (a-b)(\sum_0^{h-1} a^i b^{h-1-i})$:

$$\mathcal{D}_{L/K} = \frac{1}{\pi^{(p-1)(ll'-1)/p}} \prod_{i=1}^{p-1} \left\{ (\zeta_p^i \gamma - 1 - \gamma + 1) \sum_{j=0}^{l'-1} (\zeta_p^i \gamma - 1)^j (\gamma - 1)^{l'-1-j} \right\}$$
$$= \frac{1}{\pi^{(p-1)(ll'-1)/p}} \prod_{i=1}^{p-1} \left\{ (\zeta_p^i - 1)\gamma \sum_{j=0}^{l'-1} (\zeta_p^i \gamma - 1)^j (\gamma - 1)^{l'-1-j} \right\}.$$

Prendendo le valutazioni dei singoli fattori si ha:

$$v_L(\pi) = p;$$
$$v_L((\zeta_p^i - 1)\gamma) = v_L(\zeta_p^i - 1) = \frac{e_L}{p-1} \quad \forall i = 1, \dots p-1;$$
$$v_L((\zeta_p^i \gamma - 1)^j (\gamma - 1)^{l'-1-j}) = j v_L(\zeta_p^i \gamma - 1) + (l' - 1 - j) v_L(\gamma - 1).$$

Ma $\forall i = 1, \dots p-1$ $(\zeta_p^i \gamma - 1)$ è un coniugato di $(\gamma - 1)$, dunque le valutazioni sono uguali e $v_L(\gamma - 1) = l$; sostituendo quindi otteniamo:

$$v_L((\zeta_p^i \gamma - 1)^j (\gamma - 1)^{l'-1-j}) = jl + (l' - 1 - j)l = l(l' - 1) \quad \forall i = 1, \dots p-1.$$

Per calcolare la valutazione dell'ultima somma prendiamo $\theta \in R - \{0\}$ (dove con R indichiamo un insieme di rappresentanti di L come definito nel capitolo 1) tale che $\gamma \equiv 1 + \theta \pi_L^l$ (π_L^{l+1}) e fissiamo un certo j; allora:

$$(\zeta_p^i \gamma - 1)^j (\gamma - 1)^{l'-1-j} = (\zeta_p^i (\gamma - 1) + (\zeta_p^i - 1))^j (\gamma - 1)^{l'-1-j};$$

ma

$$v_L(\zeta_p^i (\gamma - 1)) = v_L(\gamma - 1) = l$$

e

$$v_L(\zeta_p^i - 1) = \frac{p e_K}{p-1} > l$$

quindi il termine di valutazione minore è il primo. Sostituendo dunque si ha:

$$(\zeta_p^i (\gamma - 1) + (\zeta_p^i - 1))^j \equiv \zeta_p^{ij} \theta^j \pi_L^{lj} \quad (\ mod\ \pi_L^{lj+1}),$$

da cui:

$$(\zeta_p^i \gamma - 1)^j (\gamma - 1)^{l'-1-j} \equiv \zeta_p^{ij} \theta^j \pi_L^{lj} \theta^{l'-1-j} \pi_L^{l(l'-1-j)} \quad (\ mod\ \pi_L^{lj+1+l(l'-1-j)})$$

e quindi, riscrivendo:

$$(\zeta_p^i\gamma - 1)^j(\gamma - 1)^{l'-1-j} \equiv \zeta_p^{ij}\theta^{l'-1}\pi_L^{l(l'-1)} \quad (\ mod\ \pi_L^{l(l'-1)+1}).$$

Poiché tale relazione vale $\forall j$ possiamo riscrivere la somma come:

$$\sum_{j=0}^{l'-1}(\zeta_p^i\gamma - 1)^j(\gamma - 1)^{l'-1-j} = \left(\sum_{j=0}^{l'-1}\zeta_p^{ij}\right)\theta^{l'-1}\pi_L^{l(l'-1)} \quad (\ mod\ \pi_L^{l(l'-1)+1}).$$

Osserviamo inoltre che

$$\sum_{j=0}^{l'-1}\zeta_p^{ij} = \frac{(\zeta_p^{il'} - 1)}{\zeta_p^i - 1}$$

quindi tale quantità è una unità in $\mathcal{O}_L$ per cui ha valutazione nulla. Si ha dunque:

$$v_L\left(\sum_{j=0}^{l'-1}(\zeta_p^i\gamma - 1)^j(\gamma - 1)^{l'-1-j}\right) = l(l' - 1).$$

Sommando le valutazioni dei vari pezzi otteniamo:

$$\begin{aligned} v_L(\mathcal{D}_{L/K}) &= -(p-1)(ll'-1) + (p-1)\left[\frac{e_L}{p-1} + l(l'-1)\right] \\ &= -(p-1)(ll'-1) + e_L + l(l'-1)(p-1) \\ &= (p-1) + e_L - l(p-1) \\ &= e_L - (p-1)(l-1) \\ &= pe_K - (p-1)(l-1) = (pe_K/(p-1) - l + 1)(p-1). \end{aligned}$$

Inoltre, prendendo le norme, otteniamo:

$$v_K(Disc_{L/K}) = e_L - (p-1)(l-1) = (pe_K/(p-1) - l + 1)(p-1)$$

da cui la tesi.

□

Grazie al lemma possiamo facilmente dimostrare il teorema 4.6:

Dimostrazione.

Dal lemma precedente abbiamo visto che, se $M = K(\sqrt[p]{u_l})$ allora:

$$v_M(\mathcal{D}_{M/K}) = (pe_K/(p-1) - l + 1)(p-1).$$

Inoltre, dalla proposizione 1.24 del capitolo 1 sappiamo che:

$$v_L(\mathcal{D}_{M/K}) = \sum_{s \neq id} i_G(s) = \sum_{i \geq 0}(|G_i| - 1);$$

allora, se t è il salto, $|G_i| - 1 = p - 1 \quad \forall i = 0, \dots t$ ed è 0 altrimenti; di conseguenza:

$$v_L(\mathcal{D}_{M/K}) = \sum_{i \geq 0}(|G_i| - 1) = (p-1)(t+1).$$

Uguagliando allora otteniamo:

$$(p-1)(t+1) = (pe_K/(p-1) - l + 1)(p-1)$$

da cui:

$$t + 1 = pe_K/(p-1) - l + 1$$

e dunque

$$t = pe_K/(p-1) - l.$$

□

I vari casi possono essere riassunti nel seguente corollario:

Corollario 4.8. *Sia $x \in K^*$ con $0 \leq v_K(x) < p$, $M = K(\sqrt[p]{x})$ e sia t il salto della ramificazione dell'estensione M/K. Allora:*

- *Se $0 < v_K(x) < p$ allora $t = pe/(p-1)$.*
- *Se $v_K(x) = 0$ con $l = v_K(x-1) < pe/(p-1)$ e $(l,p) = 1$, allora:*
$$t = pe/(p-1) - l.$$
- *Se $v_K(x) = 0$ e $v_K(x-1) = pe/(p-1)$, allora:*
$$t = -1 \quad \textit{(cioè l'estensione è non ramificata).}$$

Osservazione 4.9. Faremo vedere in seguito che nel caso in cui K non contenga le radici p-esime dell'unità le condizioni per il salto t dell'estensione diventano:

$$1 \leq t < pe/(p-1) \quad \text{e} \quad (t,p) = 1.$$

4.2 Estensioni con gruppo di Galois $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

A partire dai risultati ottenuti nella sezione precedente vogliamo descrivere i salti di un'estensione di Galois finita L/K totalmente ramificata e con gruppo di Galois $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.
Sia allora K un campo completo rispetto ad una valutazione discreta con $charK = 0$ e campo dei residui finito con caratteristica p. Supponiamo in aggiunta che K contenga una radice p-esima dell'unità ζ_p.
Denotiamo con $e = v_K(p)$ e con $e' = e/(p-1)$; poiché $\zeta_p \in K$ sappiamo che $v_K(\zeta_p - 1) = e'$ e quindi $e' \in \mathbb{Z}$.

Notiamo che dalle proprietà generali dei gruppi di ramificazione abbiamo che, essendo l'estensione totalmente ramificata, il primo salto in basso (e quindi anche quello in alto) è non negativo.
Inoltre, dal corollario 1.34 sappiamo che G_0/G_1 è un gruppo ciclico di ordine primo con la caratteristica di $\overline{K}$; nel nostro caso quindi $|G_0/G_1| = 1$ e 0 non è un salto dell'estensione. D'altra parte il corollario 1.35 afferma che, se $char\overline{K} = p > 0$ allora G_i/G_{i+1} è un p-gruppo abeliano elementare $\forall i \geq 1$. Segue quindi che in questo caso l'estensione può avere a priori sia uno che due salti.
Dimostriamo innanzitutto il seguente teorema:

Teorema 4.10. *Sia L/K un'estensione di Galois totalmente ramificata con gruppo di Galois $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Allora L/K ha due salti in alto della ramificazione $t^1 < t^2$ se e solo se esistono due sottoestensioni K_1/K e K_2/K di grado p con salti rispettivamente uguali a t^1 e t^2.*

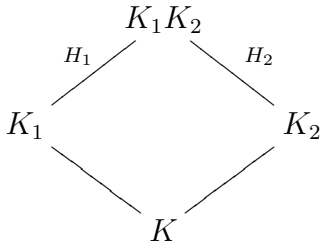
Dimostrazione.

⇒ Supponiamo che l'estensione L/K abbia due salti della ramificazione in alto t^1 e t^2. Allora la filtrazione dei gruppi di ramificazione risulta:

$$G = G^0 = \ldots = G^{t^1} \supsetneq G^{t^1+1} = \ldots = G^{t^2} \supsetneq G^{t^2+1} = \{1\}.$$

Denotiamo con $H_1 = G^{t^1+1} \cong \mathbb{Z}/p\mathbb{Z}$; allora esiste $H_2 \lhd G$ tale che $H_2 \cong G/H_1$, $H_1 \cap H_2 = \varnothing$ e $G = H_1 \times H_2$.
Chiamiamo $K_1 = Fix(H_1)$ e $K_2 = Fix(H_2)$; per la corrispondenza di Galois vale che $K_1K_2 = Fix(H_1 \cap H_2) = Fix(\{e\}) = L$, dunque $L = K_1K_2$. Vogliamo studiare la relazione tra i salti dell'estensione

L/K e i salti delle due sottoestensioni K_1/K e K_2/K.



Consideriamo l'estensione K_1/K; per la corrispondenza di Galois sappiamo che $Gal(K_1/K) \cong G/H_1$. Di conseguenza, utilizzando il la proposizione 1.51 sappiamo che

$$\forall v \geq 1 \quad (G/H_1)^v = G^v H_1/H_1.$$

Mostriamo allora che il salto della sottoestensione K_1/K è esattamente t^1. Infatti:

- $(G/H_1)^{t^1} = G^{t^1} H_1/H_1 = GH_1/H_1 = G/H_1$;
- $(G/H_1)^{t^1+1} = G^{t^1+1} H_1/H_1 = H_1/H_1 = \{1\}$.

Allo stesso modo mostriamo che il salto della sottoestensione K_2/K è esattamente t^2. Infatti, sempre per la corrispondenza di Galois sappiamo che $Gal(K_2/K) \cong G/H_2$. Allora, applicando nuovamente la proposizione 1.51 si ha che:

- $(G/H_2)^{t^2} = G^{t^2} H_2/H_2 = H_1H_2/H_2 = G/H_2$;
- $(G/H_2)^{t^2+1} = G^{t^2+1} H_2/H_2 = H_2/H_2 = \{1\}$.

Abbiamo quindi dimostrato che se L/K è un estensione con gruppo di Galois $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ e con salti in alto della ramificazione t^1 e t^2 allora esistono due sottoestensioni K_1/K e K_2/K con salti della ramificazione rispettivamente uguali a t^1 e t^2.

$\Leftarrow$ Mostriamo equivalentemente che se L/K ha un solo salto t allora tutte le sottoestensioni di grado p hanno lo stesso salto. Supponiamo quindi L/K abbia un solo salto t; in questo caso

$$G = G^1 = \ldots = G^t \neq G^{t+1} = \{1\}.$$

Sia $H \lhd G$ un sottogruppo di G di ordine p e sia $F = Fix(H)$ il campo associato. Per la corrispondenza di Galois si ha che $Gal(F/K) = G/H$. Calcoliamo il salto di F/K utilizzando la proposizione 1.51:

- $(G/H)^t = G^t H/H = G/H$;
- $(G/H)^{t+1} = G^{t+1} H/H = H/H = \{1\}$.

Di conseguenza se L/K ha un solo salto t allora tutte le sottoestensioni di L/K hanno lo stesso salto t e ciò è assurdo.

□

Dal teorema segue banalmente il seguente corollario:

Corollario 4.11. *Sia L/K un'estensione totalmente ramificata con gruppo di Galois $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Allora L/K ha un solo salto t se e solo se tutte le sottoestensioni di L/K di grado p hanno lo stesso salto.*

Per studiare quali sono le condizioni necessarie e sufficienti trattiamo i due casi separatamente:

4.2.1 Caso L/K con due salti

Abbiamo dimostrato che se L/K è un estensione con gruppo di Galois $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ e con salti in alto della ramificazione t^1 e t^2 allora esistono due sottoestensioni K_1/K e K_2/K con salti della ramificazione rispettivamente uguali a t^1 e t^2. Ciò mostra che i due salti dell'estensione L/K devono soddisfare le condizioni necessarie per essere salti di un'estensione di grado p. Vale quindi che:

$$\text{se } i = 1, 2 \text{ allora } 1 \leq t^i \leq pe' \text{ e } (t^i, p) = 1 \text{ se } t^i \neq pe'.$$

Vogliamo ora mostrare che queste condizioni sono anche sufficienti. Per fare ciò è utile distinguere il caso in cui $t^1, t^2 \neq pe'$ dal caso in cui un salto sia uguale a pe'.

- Supponiamo $1 \leq t^1 < t^2 < pe'$ con $(t^1, p) = (t^2, p) = 1$. Da quanto visto nella sezione precedente sappiamo che se u_i è una unità di K tale che $v_K(u_i - 1) = i$ con $1 \leq i < pe'$ e $(i, p) = 1$, allora $K(\sqrt[p]{u_i})/K$ è un'estensione di grado p con salto della ramificazione pari a $t = pe' - i$. Definiamo allora due estensioni di K di grado p nel modo seguente:
  - $K_1 = K(\sqrt[p]{u_l})$ con $v_K(u_l - 1) = l = pe' - t^1$; allora il K_1/K è totalmente ramificata di grado p con salto della ramificazione t^1;
  - $K_2 = K(\sqrt[p]{u_m})$ con $v_K(u_m - 1) = m = pe' - t^2$; allora il K_2/K è totalmente ramificata di grado p con salto della ramificazione t^2.

Poiché $t^1 < t^2$, si ha che $l = pe' - t^1 > pe' - t^2 = m$. Consideriamo ora il composto L di K_1 e K_2; allora L/K è banalmente un'estensione totalmente ramificata di grado p^2 con gruppo di Galois $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Vogliamo dimostrare che i salti in alto della ramificazione di L/K sono esattamente t^1 e t^2. Per fare ciò studiamo quali sono le altre sottoestensioni di L/K.
Per la teoria di Kummer sappiamo che se $\sqrt[p]{u_l}$ e $\sqrt[p]{u_m}$ generano rispettivamente K_1 e K_2 allora le altre $p-1$ estensioni sono generate dagli elementi della forma $\sqrt[p]{u_m u_l^i}$ con $i \in \{1, \dots, p-1\}$.
Calcoliamo $\forall i \in \{1, \dots, p-1\}$ il salto dell'estensione $K(\sqrt[p]{u_m u_l^i})/K$; per fare ciò dobbiamo calcolare $v_K(u_m u_l^i - 1)$.
Notiamo allora che:

- $v_K(u_m - 1) = m$;
- $v_K(u_l^i - 1) = l$ perché $(i, p) = 1$.

Di conseguenza, poiché $v_K(u_l^i - 1) \neq v_K(u_m - 1)$, si ha che

$$v_K(u_m u_l^i - 1) = min\{v_K(u_l^i - 1),\ v_K(u_m - 1)\} = v_K(u_m - 1) = m.$$

Si ha quindi che il salto delle altre $p-1$ estensioni è pari a $pe'-m$ cioè a t^2. Abbiamo quindi dimostrato che l'estensione L/K ha p sottoestensioni di grado p con salto della ramificazione pari a t^2 e un'unica sottoestensione di grado p con salto della ramificazione t^1.
D'altra parte, poiché abbiamo precedentemente dimostrato che i salti in alto di un'estensione di grado p^2 con gruppo di Galois $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ corrispondono ai salti di due sottoestensioni di grado p, si ha che nel nostro caso i salti dell'estensione L/K sono esattamente t^1 e t^2.

- Supponiamo ora che $1 \leq t^1 < pe'$ con $(t^1, p) = 1$ e $t^2 = pe'$. Definiamo allora come nel caso precedente $K_1 = K(\sqrt[p]{u_l})$ con $v_K(u_l - 1) = l = pe' - t^1$; K_1 è quindi un'estensione totalmente ramificata di Galois di grado p con salto della ramificazione pari a t^1. Inoltre, dalla proposizione 4.1 sappiamo che, se definiamo $K_2 = K(\sqrt[p]{\pi})$ dove π è un uniformizzante di K, allora K_2/K è un'estensione di Galois totalmente ramificata di grado p con salto della ramificazione pari a pe'. Se consideriamo il composto L di K_1 e K_2 allora con la stessa dimostrazione del punto precedente si ha che l'estensione L/K è totalmente ramificata con gruppo di Galois $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ e tale che i due salti in alto della ramificazione sono esattamente t^1 e t^2.

Vogliamo ora analizzare il caso in cui l'estensione L/K abbia un unico salto della ramificazione.

4.2.2 Caso L/K con un unico salto

Supponiamo che l'estensione L/K abbia un solo salto della ramificazione in alto t^1 e t^2. Allora la filtrazione dei gruppi di ramificazione risulta:

$$G = G^0 = \ldots = G^t \supsetneq G^{t+1} = \{1\}.$$

Abbiamo visto nel teorema 4.10 che se L/K ha un unico salto t allora tutte le sue sottoestensioni di grado p hanno come salto lo stesso t. Di conseguenza affiché t sia l'unico salto della ramificazione di un'estensione L/K con gruppo di Galois $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ è necessario che t soddisfi le condizioni per essere salto di un'estensione di grado p. Vale quindi la condizione necessaria:

$$1 \leq t \leq pe' \text{ e } (t,p) = 1 \text{ se } t \neq pe'.$$

Vogliamo vedere se tale condizione è anche sufficiente. In realtà ciò dipende dalla dimensione di $\overline{K}$ come spazio vettoriale su $\mathbb{F}_p$.

Supponiamo infatti di voler realizzare un'estensione L/K totalmente ramificata di grado p^2 con gruppo di Galois $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ e con un unico salto della ramificazione t. Distinguiamo due casi:

1. Supponiamo $1 \leq t < pe'$ e $(t,p) = 1$.
   Consideriamo allora u_m e v_m due unità di K tali che

   $$v_K(u_m - 1) = v_K(v_m - 1) = m$$

   con $m = pe' - t$. Se indichiamo con $K_1 = K(\sqrt[p]{u_m})$ e $K_2 = K(\sqrt[p]{v_m})$ si ha che K_1/K e K_2/K sono due estensioni totalmente ramificate di grado p con salto della ramificazione uguale a t.
   Denotiamo ora con L il composto delle due estensioni K_1 e K_2; allora L/K è un'estensione totalmente ramificata di grado p^2 con gruppo di Galois $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Per imporre che L/K abbia un unico salto dobbiamo imporre che le altre $p-1$ sottoestensioni di L/K abbiano salto della ramificazione pari a t. Come prima sappiamo che le altre sottoestensioni di L/K sono della forma $K(\sqrt[p]{u_m v_m^i})$ $\forall i = 1, \ldots p-1$.
   Dobbiamo quindi calcolare $v_K(u_m v_m^i - 1)$ e imporre $v_K(u_m v_m^i - 1) = m$ $\forall i = 1, \ldots p-1$.
   Scriviamo u_m e v_m più esplicitamente come:

   - $u_m = 1 + a\pi^m$ con $a \in U_K$
   - $v_m = 1 + b\pi^m$ con $b \in U_K$.

Indichiamo con $\overline{a}$ e $\overline{b}$ le rispettive proiezioni di a e b nel campo dei residui $\overline{K}$; poiché stiamo supponendo che $v_K(u_m - 1) = v_K(v_m - 1) = m$ abbiamo che $\overline{a}$ e $\overline{b}$ sono entrambi diversi da 0. Allora

$$u_m v_m^i = (1 + a\pi^m)(1 + b\pi^m)^i = 1 + (\overline{a} + i\overline{b})\pi^m \quad (\pi^{m+1}).$$

Di conseguenza $v_K(u_m v_m^i - 1) = m$ se e solo se $\overline{a} + i\overline{b} \neq 0$; poiché tale relazione deve valere $\forall i = 0, \dots p - 1$ ciò significa che $\overline{a}$ e $\overline{b}$ sono due elementi non nulli di $\overline{K}$ indipendenti su $\mathbb{F}_p$.
Tuttavia se $\overline{K} = \mathbb{F}_p$ tale condizione non è mai verificata (in quanto presi due elementi qualsiasi di $\mathbb{F}_p$ sono sempre dipendenti tra loro).
Abbiamo quindi dimostrato la seguente proposizione:

Proposizione 4.12. *Se $\overline{K} = \mathbb{F}_p$ allora non esistono estensioni totalmente ramificate con gruppo di Galois $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ e con unico salto in alto della ramificazione t tale che $1 \leq t < pe'$ e $(t, p) = 1$.*

2. Supponiamo ora $t = pe'$. Dalla proposizione 4.1 sappiamo che se prendiamo $M = K(\sqrt[p]{x})$ con $0 < v_K(x) < p$, allora M/K è totalmente ramificata con salto della ramificazione $t = pe/(p-1)$. Inoltre, poiché se $(i, p) = 1$ si ha che $K(t) = K(t^i)$, possiamo sempre scegliere un generatore un modo tale che $v_K(x) = 1$.
Consideriamo allora due estensioni $K_1 = K(\sqrt[p]{a\pi})$ e $K_2 = K(\sqrt[p]{b\pi})$ con $a, b \in U_K$. Sappiamo che tali estensioni sono totalmente ramificate di grado p con salto della ramificazione pari a pe'. Consideriamo ora l'estensione composta L/K con $L = K_1K_2$; per imporre che L/K abbia come unico salto pe' dobbiamo mostrare che anche le altre sottoestensioni hanno lo stesso salto. Le altre estensioni sono generate dagli elementi della forma $\sqrt[p]{a\pi(b\pi)^i}$ con $i = 1, \dots, p-1$. Osserviamo tuttavia che $(a\pi)(b\pi)^{p-1} = ab^{p-1}\pi^p$, quindi $K(\sqrt[p]{a\pi(b\pi)^{p-1}}) = K(\sqrt[p]{ab^{p-1}})$ e $v_K(ab^{p-1}) = 0$. Di conseguenza la sottoestensione $K(\sqrt[p]{ab^{p-1}})$ è totalmente ramificata ma il salto della ramificazione è diverso da pe'.
Ciò dimostra la proposizione seguente:

Proposizione 4.13. *Non esistono estensioni totalmente ramificate con gruppo di Galois $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ e con unico salto in alto della ramificazione $t = pe'$.*

Capitolo 5

Il teorema di Miki

Sia K un campo completo rispetto ad una valutazione discreta v_K con $charK = 0$ e $char\overline{K} = p > 0$. Supponiamo inoltre che il campo dei residui $\overline{K}$ sia finito (in particolare quindi perfetto).

Vogliamo determinare in generale le condizioni necessarie e sufficienti affinché data una m-pla di interi $\{t^1, \dots, t^m\}$ esista un'estensione L/K ciclica, totalmente ramificata di grado p^m e tale che i salti di ramificazione in alto siano proprio $t^1, \dots t^m$.

Osserviamo che nel caso in cui il campo K non contenga radici p-esime dell'unità la trattazione è più semplice, e ciò dipende principalmente dal fatto che in questo caso il gruppo delle unità U_K^1 è uno $\mathbb{Z}_p$ modulo libero di rango il grado dell'estensione. Tale caso è stato infatti il primo ad essere risolto completamente dal matemitico tedesco E.Maus.
Solo molti anni più tardi il matematico giapponese H.Miki è giunto alla risoluzione completa del teorema. Nel caso generale tuttavia le condizioni sui salti saranno più complicate e saranno legate ad una particolare fattorizzazione della massima radice p^s-esima dell'unità contenuta in K.
In questo capitolo ci occupiamo di enunciare i vari risultati.

5.1 Caso $\zeta_p \notin K$

Iniziamo quindi con il trattare il caso in cui il campo K non contenga radici p-esime dell'unità. Nelle ipotesi precedenti, poniamo $e' = e/(p-1)$.
Osserviamo che se K non contiene le radici p-esime dell'unità allora e' non è necessariamente intero.

Denotiamo con

$$f(t) = min\{pt,\ t+e\} = \begin{cases} pt & \text{se } t \le e' \\ t+e & \text{se } t > e' \end{cases}$$

e indichiamo con f^k la k-esima iterata della funzione f.
Vale allora il seguente teorema:

Teorema 5.1 (E.Maus)**.** *Sia $T = \{t^1 \le \ldots \le t^m\}$ un insieme finito di numeri naturali. Allora esiste un'estensione ciclica L/K totalmente ramificata di grado p^m con salti della ramificazione $t^1, \ldots t^m$ se e solo se:*

1. *$t^{i+1} \ge f(t^i)$ se $i = 1, \ldots m-1$ e*
2. *se $t^i = f^h(t')$ con $0 < t' \le pe/(p-1)$ e $p \nmid t'$, allora anche $t' \in T$.*

Tale teorema può essere enunciato nella seguente formulazione equivalente, che rende le condizioni sui salti più esplicite:

Teorema 5.2. *Sia $\{t^1 \le \ldots \le t^m\}$ un insieme finito di numeri naturali. Allora esiste un'estensione ciclica L/K totalmente ramificata di grado p^m con salti della ramificazione $t^1, \ldots t^m$ se e solo se valgono le tre condizioni seguenti:*

1. *$1 \le t^1 < e'p$ e $(t^1, p) = 1$;*
2. *se $t^i < e'$ allora t^{i+1} soddisfa una delle due condizioni seguenti:*
   - *$t^{i+1} = pt^i$;*
   - *$pt^i < t^{i+1} < pe/(p-1)$ e $(p, t^{i+1}) = 1$;*
3. *se $t^i \ge e'$; allora $t^{i+1} = t^i + e$.*

Nei prossimi due capitoli daremo una dimostrazione completa del teorema, dimostrando separatamente che le condizioni precedenti sono sia necessarie che sufficienti.

Analizziamo ora il caso in cui $\zeta_p \in K$; per fare ciò abbiamo tuttavia bisogno di un lemma preliminare.

5.2 Lemma di decomposizione

Sia K un campo completo rispetto al una valutazione discreta v_K; supponiamo $charK = 0$, $char\overline{K} = p$ e infine che il campo dei residui sia finito. Supponiamo inoltre che $\zeta_p \in K$ dove con ζ_p indichiamo una radice p-esima primitiva dell'unità. Indichiamo con $e = v_K(p)$ e con $e' = e/(p-1)$. Vale allora il seguente lemma:

Lemma 5.3. *(Lemma di decomposizione) Sia α un elemento di U_K^1 tale che $1 \le v_K(\alpha-1) < e'p$ e sia l l'intero non negativo tale che $p^l \parallel v_K(\alpha-1)$. Allora possiamo scrivere:*

$$\alpha = \xi_l \xi_{l-1}^p \dots \xi_1^{p^{l-1}} \xi_0^{p^l}$$

dove $\xi_l, \xi_{l-1}, \dots, \xi_0$ sono $(l+1)$ elementi di U_K^1 che soddifano le seguenti relazioni (A) e (B) :

(A) *$\forall i$ tale che $0 \le i \le l$, vale una delle 3 condizioni seguenti:*

1. $\xi_i = 1$
2. $v_K(\xi_i - 1) < e'p$ *e* $v_K(\xi_i - 1) \not\equiv 0 \ (p)$
3. $v_K(\xi_i - 1) = e'p$ *e* $\xi_i \notin K^p$

(B) $p^{l-i} v_K(\xi_i - 1) < p^{l-j} v_K(\xi_j - 1)$ *$\forall$ coppia (i,j) con $0 \le i < j \le l$ tale che* $\xi_i \neq 1$ *e* $\xi_j \neq 1$.

Inoltre, se $\alpha \notin K^p$, allora i $v_K(\xi_i - 1)$ sono univocamente determinati da α per $i = 0, 1, \dots l$.

Dimostrazione. Dimostriamo la proposizione per induzione su l.

- $l = 0$
  Sappiamo per ipotesi che $p \nmid v_K(\alpha - 1)$; allora α è un elemento di U_K^1 tale che $v_K(\alpha - 1) < e'p$ e $v_K(\alpha - 1) \not\equiv 0 \ (p)$. Inoltre $\alpha = \alpha^{p^l}$ (in quanto $l = 0$), dunque possiamo prendere semplicemente $\xi_0 = \alpha$.

- Supponiamo $l \ge 1$.
  Possiamo allora scrivere $\alpha = \xi_l \beta^p$ con $\xi_l,\ \beta \in U_K^1$, dove ξ_l soddisfa la condizione (A) (ξ_l è un elemento di U_K^1 tale che $v_K(\xi_l - 1)$ sia il massimo nell'espressione $\alpha = \xi_l \beta^p$). Infatti:

  1. Se $\alpha \in K^p$ allora $\exists \beta \in K$ tale che $\beta^p = \alpha$; in particolare $\beta \in U_K^1$ perché $\alpha \in U_K^1$ per ipotesi. Allora possiamo prendere $\xi_l = 1$.
  2. Supponiamo che $\alpha \notin K^p$ e scriviamo $\alpha = \xi_l \beta^p$ (con β eventualmente uguale ad 1). Vogliamo dimostrare che $v_K(\xi_l - 1)$ soddisfa una delle condizioni di (A).
     - Poiché $\alpha \notin K^p$ sicuramente $\xi_l \neq 1$.
     - Supponiamo per assurdo che $v_K(a_l - 1) = t > e'p$. Allora

$$t - e = t - e'(p-1) > e'p - e'p + e' = e'$$

e sappiamo che in generale se $m > e'$ vale $(U_K^m)^p = U_K^{m+e}$.
Nel nostro caso dunque $(U_K^{t-e})^p = U_K^t$, quindi $\exists \gamma \in U_K^{t-e}$ tale che $\gamma^p = \xi_l$, da cui $\alpha \in K^p$, che è assurdo. Di conseguenza $v_K(\xi_l - 1) \leq e'p$.

- Se $v_K(\xi_l - 1) = e'p$ allora $\xi_l \notin K^p$ perché per ipotesi $\alpha \notin K^p$ e dunque è verificata la condizione 3. del punto (A).
- Supponiamo che $v_K(\xi_l - 1) < e'p$ e supponiamo per assurdo che $v_K(\xi_l - 1) \equiv 0 \ (p)$; allora $v_K(a_l - 1) = pt$ con $t < e'$.
Di conseguenza, poiché elevare alla p è un isomorfismo tra U_K^t/U_K^{t+1} e e U_K^{pt}/U_K^{pt+1} se $t < e'$, allora ξ_l è una potenza p-esima, il che è assurdo. Si ha quindi che $v_K(\xi_l - 1) \not\equiv 0 \ (p)$.

Osservazione 5.4. Notiamo che, se $\xi_l \neq 1$, allora $v_K(\xi_l - 1) \geq v_K(\beta^p - 1)$. Infatti per ipotesi $e'p > v_K(\alpha - 1)$, di conseguenza:

- Se $\xi_l = 1$ oppure $v_K(\xi_l - 1) = e'p$, allora

$$e'p > v_K(\alpha - 1) \geq min\{v_K(\xi_l - 1),\ v_K(\beta^p - 1)\},$$

dunque $v_K(\xi_l - 1) > v_K(\beta^p - 1)$.

- Se $v_K(\xi_l - 1) < e'p$ e $v_K(\xi_l - 1) \not\equiv 0 \ (p)$ allora necessariamente si ha che $v_K(\xi_l - 1) \neq v_K(\beta^p - 1)$ perché $v_K(\beta^p - 1) = pt$ per un qualche $t < e'$. Se per assurdo $v_K(\xi_l - 1) < v_K(\beta^p - 1)$, allora si avrebbe $v_K(\xi_l - 1) = v_K(\alpha - 1)$ che per ipotesi è divisibile per p, e ciò è assurdo.

Di conseguenza vale $v_K(\alpha - 1) = v_K(\beta^p - 1) < e'p$ e quindi, poiché $v_K(\beta^p - 1) = pv_K(\beta - 1)$, si ha:

$$v_K(\beta - 1) = \frac{1}{p}\, v_K(\alpha - 1)$$

D'altra parte, poiché $1 \leq v_K(\alpha - 1) < e'p$ e $p^l \parallel v_K(\alpha - 1)$, segue:

$$1 \leq v_K(\beta - 1) < e' \quad e \quad p^{l-1} \parallel v_K(\beta - 1).$$

Applichiamo l'ipotesi induttiva a β; possiamo dunque scrivere:

$$\beta = \xi_{l-1}\xi_{l-2}^p \dots \xi_0^{p^{l-1}}$$

dove $\xi_{l-1}, \dots \xi_0$ sono elementi di U_K^1 che soddisfano la condizione (A) e la seguente condizione (B'):

(B') $p^{l-1-i}v_K(\xi_i - 1) < p^{l-1-j}v_K(\xi_j - 1)$
$\forall$ coppia (i,j) con $0 \le i < j \le l-1$ tale che $\xi_i \neq 1$ e $\xi_j \neq 1$.

Di conseguenza, $\alpha = \xi_l \xi_{l-1}^p \dots \xi_1^{p^{l-1}} \xi_0^{p^l}$. Moltiplicando ambo i membri di (B') per p, otteniamo la condizione (B''):

(B'') $p^{l-i}v_K(\xi_i - 1) < p^{l-j}v_K(\xi_j - 1)$
$\forall$ coppia (i,j) con $0 \le i < j \le l-1$ tale che $\xi_i \neq 1$ e $\xi_j \neq 1$.

Vogliamo ora paragonare anche l'elemento ξ_l.
Osserviamo che, se $\xi_l = 1$, non c'è nulla da dimostrare.
Supponiamo dunque $\xi_l \neq 1$ e sia j il massimo indice tale che $\xi_j \neq 1$.
Distinguiamo vari casi:

- Se $v_K(\xi_l - 1) > p^{l-j}v_K(\xi_j - 1)$, allora la condizione (B) vale per questa disuguaglianza e per (B'').
  Infatti se k è un altro indice con $\xi_k \neq 1$ e $0 \le k < j \le l-1$ allora

  $$v_K(\xi_l - 1) > p^{l-j}v_K(\xi_j - 1) > p^{l-k}v_K(\xi_k - 1),$$

  dunque vale la condizione (B).
- Se $v_K(\xi_l - 1) < p^{l-j}v_K(\xi_j - 1)$, allora (poiché gli ξ_j per ipotesi induttiva soddisfano la condizione per cui $v_K(\xi_j - 1) \le e'p$), si ha $v_K(\xi_l - 1) < v_K(\xi_j^{p^{l-j}} - 1)$, da cui

  $$v_K(\xi_l - 1) = v_K(\xi_l \xi_j^{p^{l-j}} - 1).$$

  Allora, a meno di rimpiazzare ξ_l con $\xi_l \xi_j^{p^{l-j}}$, possiamo prendere $\xi_j = 1$.
- Se $v_K(\xi_l - 1) = p^{l-j}v_K(\xi_j - 1)$, si ha $v_K(\xi_l - 1) \equiv 0 \ (p)$, da cui $v_K(\xi_l - 1) = e'p$ e $\xi_l \notin K^p$ dalla condizione (A).
  Poiché $v_K(\xi_j^{p^{l-j}} - 1) \ge v_K(\xi_l - 1) = e'p$, allora $v_K(\xi_l \xi_j^{p^{l-j}} - 1) \ge e'p$.
  D'altra parte $\xi_l \xi_j^{p^{l-j}} \notin K^p$, da cui $v_K(\xi_l \xi_j^{p^{l-j}} - 1) \le e'p$ (in quanto in generale se $m > e'p$ allora $U_K^m \subset K^p$).
  Di conseguenza $v_K(\xi_l \xi_j^{p^{l-j}} - 1) = e'p$ e $\xi_l \xi_j^{p^{l-j}} \notin K^p$, quindi a meno di rimpiazzare ξ_l con $\xi_l \xi_j^{p^{l-j}}$ possiamo porre $\xi_j = 1$.

Continuando tale procedura (che termina in quanto gli ξ_j sono in numero finito) possiamo prendere $\xi_l,\ \xi_{l-1} \dots \xi_0$ in modo che valgano le condizioni (A) e (B).

Vogliamo ora dimostrare l'unicità degli ordini dei fattori della decomposizione precedente nel caso in cui $\alpha \notin K^p$.
Sia allora $\alpha = \eta_l \eta_{l-1}^p \dots \eta_0^{p^l}$ un'altra espressione di α che soddisfi le condizioni (A) e (B). Poiché $\alpha \notin K^p$, si ha banalmente $\xi_l \neq 1$ e $\eta_l \neq 1$.
Notiamo che in modo ovvio $v_K(\xi_0 - 1) = v_K(\eta_0 - 1)$. Infatti dalla condizione (B) sappiamo che $p^l v_K(\xi_0 - 1) < p^{l-i} v_K(\xi_i - 1)$ $\forall i$ tale che $\xi_i \neq 1$, e lo stesso vale per η_0, dunque

$$v_K(\alpha - 1) = p^l v_K(\xi_0 - 1) = p^l v_K(\eta_0 - 1),$$

da cui $v_K(\xi_0 - 1) = v_K(\eta_0 - 1)$.
Supponiamo per assurdo che esista $1 \leq i \leq l$ tale che $v_K(\xi_i - 1) < v_K(\eta_i - 1)$ e $v_K(\xi_j - 1) = v_K(\eta_j - 1)$ $\forall j$ tale che $0 \leq j < i$. Allora:

$$(\xi_i \eta_i^{-1})^{p^{l-i}} \equiv \{(\xi_{i-1}^{-1}\eta_{i-1})(\xi_{i-2}^{-1}\eta_{i-2})^p \dots (\xi_0^{-1}\eta_0)\}^{p^{l-i+1}} \quad (\pi^{\lambda p^{l-i}+1})$$

dove con π indichiamo un uniformizzante di K e $\lambda = v_K(\xi_i - 1)$. Di conseguenza, $p^{l-i}\lambda \equiv 0$ (p^{l-i+1}), da cui otteniamo che $\lambda \equiv 0$ (p) .
Poiché $\alpha \notin K^p$, necessariamente $i = l$ e $\lambda = e'p$, dunque $\eta_l = 1$ che è assurdo.
Quindi, se $\alpha \notin K^p$, gli ordini dei fattori della decomposizione sono univocamente determinati.

□

Osservazione 5.5. Per avere l'unicità degli ordini, l'ipotesi $\alpha \notin K^p$ del lemma precedente è essenziale; per mostrare ciò consideriamo il seguente controesempio.

Sia $L/\mathbb{Q}_p$ un'estensione totalmente ramificata di grado e, con L che contenga una radice p-esima primitiva dell'unità ζ ed $e' = e/(p-1) > p$ ed $(e', p) = 1$.
Una tale estensione può essere ottenuta nel modo seguente:
Sia $K = \mathbb{Q}_p(\zeta)$ con $p \neq 2$; allora $K/\mathbb{Q}_p$ è un'estensione totalmente ramificata di grado $p-1$ e $\pi_K = \zeta - 1$ è un uniformizzante di K. Sia ora $n = p+1$ e sia α una radice del polinomio $x^n - \pi_K$. Allora, se $L = K(\alpha)$, l'estensione L/K è totalmente ramificata di grado n; di conseguenza, utilizzando le proprietà delle torri, $L/\mathbb{Q}_p$ è un'estensione totalmente ramificata di grado $e = (p-1)(p+1)$ ed $e' = e/(p-1) = p+1$.
Sia ora π_L un uniformizzante del campo L. Consideriamo $\xi_1 = 1 + \pi_L^{e'+1}$, $\xi_2 = 1 + \pi_L$ e prendiamo $\alpha = \xi_1^p \xi_2^{p^2}$. Calcoliamo $v_L(\alpha - 1)$:

- $v_L(\xi_1^p - 1) = min\{p(e'+1), e + e' + 1\} = e + e' + 1 = pe' + 1$;
- $v_L(\xi_2^{p^2} - 1) = p^2$;

dunque $v_L(\alpha - 1) = min\{pe' + 1, p^2\} = p^2$. Applichiamo il lemma ad α con $l = 2$. Allora ξ_1 e ξ_2 sono 2 elementi che soddisfano le condizioni (A) e (B) del lemma. Infatti:

- $v_L(\xi_1 - 1) = e' + 1$, quindi $1 \leq v_L(\xi_1 - 1) < e'p$ e $v_L(\xi_1 - 1) \not\equiv 0 \ (p)$ (perché $p \neq 2$);
- $v_L(\xi_2 - 1) = 1$;
- $p^2 v_L(\xi_2 - 1) = p^2 < p \ v_L(\xi_1 - 1) = p(e' + 1) = p^2 + 2p$.

D'altra parte, se prendiamo $\eta_1 = \zeta\xi_1$, allora $\eta_1^p = \xi_1^p$, quindi possiamo scrivere α come $\alpha = \eta_1^p \xi_2^{p^2}$, e anche η_1 e ξ_2 soddisfano le condizioni (A) e (B) del lemma. Infatti:

- $v_L(\eta_1 - 1) = v_L(\zeta\xi_1 - 1) = min\{v_L(\zeta - 1), v_L(\xi_1 - 1)\} = e' = p + 1$, dunque $1 \leq v_L(\eta_1 - 1) < e'p$ e $v_L(\eta_1) \not\equiv 0 \ (p)$;
- $p^2 v_L(\xi_2 - 1) = p^2 < p \ v_L(\eta_1 - 1) = pe' = p^2 + p$.

Tuttavia in questo caso gli ordini dei fattori non si conservano. Infatti

$$v_L(\xi_1 - 1) = e' + 1 \neq v_L(\eta_1 - 1) = e'.$$

Definizione 5.1. $\forall \alpha$ tale che $1 \leq v_K(\alpha - 1) < e'p$ e $\alpha \notin K^p$, poniamo:

$$\lambda_i(\alpha; K) = \lambda_i(\alpha) = v_K(\xi_i - 1) \quad \forall \ i = 0, 1 \ldots l$$

dove $\xi_l, \xi_{l-1} \ldots \xi_0$ sono $(l + 1)$ elementi di U_K^1 che soddisfano le condizioni del lemma.

Definizione 5.2. Suppiamo che $\zeta_1 \in K$. Sia l un intero non negativo tale che $p^l \parallel v_K(\zeta_s - 1)$, dove ζ_s è la radice p^s-esima primitiva dell'unità tale che $\zeta_s \in K$ e $\zeta_{s+1} \notin K$. Poniamo allora:

$$I(K) = (s; \lambda_0, \lambda_1, \ldots \lambda_l)$$

dove $\lambda_i = \lambda_i(\zeta_s; K)$ per $i = 0, 1, \ldots l$. Dato che s, l e λ_i sono indipendenti dalla scelta di ζ_s, $I(K)$ è un invariante di K.

Osservazione 5.6. Tale invariante, che avrà un ruolo fondamentale nella risoluzione del problema sui salti della ramificazione nel caso generale, non è sempre facile da calcolare. Nell'ultimo capitolo mostreremo che in alcuni casi c'è un metodo abbastanza esplicito per calcolare l'invariante $I(K)$.

5.3 Caso $\zeta_p \in K$

Sia K un campo completo rispetto al una valutazione discreta v_K; supponiamo $charK = 0$, $char\overline{K} = p$ e che il campo dei residui sia finito. Supponiamo inoltre che le radici p-esime dell'unità siano contenute in K e indichiamo con $e = v_K(p)$ e con $e' = e/(p-1)$. Indichiamo poi con ζ_i alcune radici p^i-esime dell'unità tali che $\zeta_{i+1}^p = \zeta_i \ \forall i \geq 1$ e sia $s = s(K)$ l'intero tale che $\zeta_s \in K$ e $\zeta_{s+1} \notin K$.

Sia inoltre $I(K) = (s; \lambda_0, \lambda_1, \dots \lambda_l)$ l'invariante del campo definito nella sezione precedente.

Fissiamo $\{t^1, \dots, t^m\}$ una m-pla di interi distinti e poniamo $t^i = 0 \forall i \leq 0$. Definiamo la seguente condizione $C(j)$ che dipende soltanto dall'invariante $I(K)$ e dall'insieme $\{t^1, \dots, t^m\}$:

$C(j)$ Esiste un sottoinsieme T di $\{0, 1 \dots l\}$ tale che:

- $t^{j-i} = \lambda_{l-i} \quad \forall i \in T$;
- $t^{j-i} < \lambda_{l-i} \quad \forall i \in \{0, 1 \dots l\} - T$,

e la cardinalità dell'insieme T è 1 se $p \neq 2$ e dispari se $p = 2$.
Vale allora il seguente teorema:

Teorema 5.7 (teorema di Miki)**.** *Sia K un campo completo che soddisfi le proprietà descritte sopra e sia $\{t^1, \dots, t^m\}$ una m-pla di interi distinti. Allora esiste un'estensione L/K ciclica totalmente ramificata di grado p^m con salti della ramificazione $\{t^1, \dots, t^m\}$ se e solo valgono le seguenti condizioni:*

(a) t^1 soddisfa una delle due condizioni seguenti:

- $1 \leq t^1 < e'p$ *e* $t^1 \not\equiv 0(p)$*;*
- $t^1 = e'p$.

(b) Se $t^i < e'$, allora t^{i+1} soddisfa una delle 3 condizioni seguenti:

- $t^{i+1} = pt^i$*;*
- $pt^i < t^{i+1} < e'p$ *e* $t^{i+1} \not\equiv 0(p)$*;*
- $t^{i+1} = e'p$.

(c) Se $t^i \geq e'$, allora $t^{i+1} = t^i + e$.

(d) Poniamo $t^i = 0$ per ogni $i \leq 0$ e n, se esiste, il minimo intero con $1 \leq n \leq m$ tale che $t^n \geq e'$. Allora:

- *Se $\overline{K} = \mathbb{F}_p$ e vale la condizione $C(j)$ vale per un certo $1 \leq j \leq m$ allora $j \geq n - s + 1$ e $m \leq j + s - 1$.*
- *Se $\overline{K} = \mathbb{F}_q$ con $q = p^f$ e vale la seguente condizione:*

$$t^j = \lambda_l = pe',\ t^{j-1} < e' \text{ e } t^{j-i} < \lambda_{l-i}\ \forall i \in \{1, \ldots, l\}$$

per qualche $j \in \{1, \ldots, m\}$, allora $j = n$ e $m \leq n + s - 1$.

Ricordiamo ora la seguente definizione:

Definizione 5.3. Un'estensione di Galois K_∞ di K è detta $\mathbb{Z}_p$-estensione di K se il gruppo di Galois $G(K_\infty/K)$ è topologicamente isomorfo al gruppo additivo $\mathbb{Z}_p$ dell'anello degli interi p-adici.

Il seguente risultato di Maus è il caso speciale per $l = 0$ del teorema principale:

Corollario 5.8. *Supponiamo che $\{t^1, t^2, \ldots\}$ un insieme di interi che soddisfa le proprietà (a), (b) e (c) del teorema di Miki. Sia n il minimo intero tale che $t^n \geq e'$. Supponiamo che $v_K(\zeta_s - 1) \not\equiv 0\ (p)$. Allora:*

- *Se $\overline{K} = \mathbb{F}_p$, allora valgono le due condizioni seguenti:*
  1. *Supponiamo che $v_K(\zeta_s - 1) = t^j$ per qualche j. Allora necessariamente $n - s + 1 \leq j \leq n$. Inoltre esiste un'estensione ciclica totalmente ramificata K_m di K di grado p^m tale che i salti della ramificazione siano $\{t^1, t^2, \ldots, t^m\} \iff m \leq j + s - 1$.*
  2. *Se $v_K(\zeta_s - 1) \notin \{t^1, \ldots, t^n\}$ allora esiste una $\mathbb{Z}_p$-estensione K_∞ totalmente ramificata di K tale che l'insieme dei salti in alto della ramificazione sia $\{t^1, t^2, \ldots\}$.*
- *Se $\overline{K} \neq \mathbb{F}_p$, allora esiste una $\mathbb{Z}_p$-estensione K_∞ totalmente ramificata di K tale che l'insieme dei salti in alto della ramificazione sia $\{t^1, t^2, \ldots\}$.*

Corollario 5.9. *Sia K un campo che soddisfi le ipotesi dei teoremi precedenti; supponiamo in aggiunta che $\overline{K} = \mathbb{F}_p$. Sia $\{t^1 \ldots t^m\}$ una m-pla di numeri interi che soddisfino le condizioni (a), (b) o (c) del teorema di Miki e supponiamo che valga una delle due condizioni seguenti:*

1. *$\{\lambda_0, \ldots, \lambda_l\} \cap \{t^1, \ldots, t^m\} = \varnothing$ oppure*
2. *$t_1 > \lambda_l$.*

Allora $\exists$ una $\mathbb{Z}_p$-estensione K_∞ totalmente ramificata di K tale che l'insieme dei salti in alto della ramificazione sia $\{t^1, t^2, \ldots\}$.

Nei capitoli successivi daremo una dimostrazione completa del risultato di Miki, fornendo nei vari casi una costruzione esplicita del sottogruppo normico associato all'estensione con salti della ramificazione cercati.

Capitolo 6

Condizioni necessarie

In questo capitolo vogliamo dare una dimostrazione del fatto che le condizioni enunciate nel teorema di Maus e nel teorema di Miki siano necessarie. Per fare ciò dobbiamo dimostrare un teorema preliminare che dà una caratterizzazione di salti della ramificazione di un'estensione L/K in termini del sottogruppo normico associato. Tale teorema sarà usato più volte anche nella dimsotrazione della sufficienza delle condizioni.

6.1 Caratterizzazione dei salti della ramificazione

Teorema 6.1. *Sia K un campo completo rispetto ad una valutazione discreta con $charK = 0$ e campo dei residui finito di caratteristica p. Sia L/K un'estensione ciclica totalmente ramificata di grado p^m . Indichiamo con $t^1, \dots t^m$ i salti in alto dell'estensione L/K.*
Allora vale vale:

$$t^i = min\{j \in \mathbb{N} \mid U^{(j+1)} \subseteq N_{L/K}(L^*)K^{*p^i}\} \qquad \forall i = 1, \dots m.$$

Per dimostrare il teorema precedente dobbiamo approfondire alcune proprietà dei gruppi normici nel caso in cui $|\overline{K}| < +\infty$:

6.2 Gruppi normici nel caso $|\overline{K}| < +\infty$

Sia K un campo completo rispetto ad una valutazione discreta v_K; supponiamo in aggiunta che il campo dei residui $\overline{K}$ sia finito.

Sia inoltre L/K un'estensione di Galois totalmente ramificata e finita con gruppo di Galois G. Indichiamo per brevità con $N = N_{L/K}$. Dal corollario 2.19 abbiamo visto che per le estensioni totalmente ramificate vale $U_K/NU_L \cong K^*/NL^*$.
Vogliamo descrivere la filtrazione di U_K/NU_L attraverso le immagini degli U_K^n. Dalla proposizione 2.21 sappiamo che esiste la seguente successione esatta:

$$0 \longrightarrow G_{\psi(n)}/G_{\psi(n)+1} \xrightarrow{\vartheta} U_L^{\psi(n)}/U_L^{\psi(n)+1} \xrightarrow{N_n} U_K^n/U_K^{n+1}$$

dove N_n è definita da un polinomio additivo (rispettivamente moltiplicativo) se $n \geq 1$ (rispttivamente se $n = 0$).
Si può allora dimostrare che vale la proposizione seguente:

Proposizione 6.2. *Il gruppo $U_K^n/U_K^{n+1}NU_L^{\psi(n)}$ è isomorfo a $G_{\psi(n)}/G_{\psi(n)+1}$.*

(una dimostrazione dettagliata di tale proposizione può essere trovata su [Ser]).

Poniamo allora $h_n = [G_{\psi(n)} : G_{\psi(n)+1}]$. Dalla proposizione precedente segue in modo ovvio il corollario:

Corollario 6.3. $[U_K^n : U_k^{n+1}U_L^{\psi(n)}] = h_n$

Corollario 6.4. *Il gruppo $NU_L^{\psi(n)}$ è un sottogruppo di U_K^n di indice finito. Se denotiamo con v_n tale indice allora $v_n = 1$ per n sufficientemente grande; inoltre v_n divide $h_n v_{n+1}$ e l'uguaglianza si ha $\iff$ l'omomorfismo canonico*

$$\alpha_n : U_K^{n+1}/NU_L^{\psi(n+1)} \longrightarrow U_K^n/NU_L^{\psi(n)}$$

è iniettivo.

Dimostrazione. Utilizzando il corollario 2.24 sappiamo che, se $G_{\psi(n)} = \{1\}$, allora $N(U_L^{\psi(n)}) = U_K^n$; di conseguenza $N(U_L^{\psi(n)}) = U_K^n$ per n sufficientemente grande.
D'altra parte vale la seguente successione esatta:

$$U_K^{n+1}/NU_L^{\psi(n+1)} \xrightarrow{i} U_K^n/NU_L^{\psi(n)} \xrightarrow{\pi} U_K^n/U_K^{n+1}NU_L^{\psi(n)} \longrightarrow 0$$

Tale successione ci dice che, se v_{n+1} è finito, allora lo è anche v_n e inoltre $v_n \mid v_{n+1}h_n$.
Dalla successione precedente sappiamo che $ker\pi \cong Im(U_K^{n+1}/NU_L^{\psi(n+1)})$ e che π è surgettiva; di conseguenza:

$$U_K^n/U_K^{n+1}NU_L^{\psi(n)} \cong (U_K^n/NU_L^{\psi(n)})/Im(U_K^{n+1}/NU_L^{\psi(n+1)}).$$

Quindi, se indichiamo con $d_{n+1} = |Im(U_K^{n+1}/NU_L^{\psi(n+1)})|$, si ha:

$$h_n = v_n/d_{n+1} \quad \text{con} \quad d_{n+1} \mid v_{n+1}, \quad \text{e} \quad d_{n+1} = v_{n+1} \quad \Longleftrightarrow \quad i \text{ iniettivo.}$$

Allora:

$$v_n \mid v_{n+1}h_n, \quad \text{e si ha l'uguaglianza} \quad \Longleftrightarrow \quad i \text{ è iniettivo.}$$

□

Corollario 6.5. *L'intero $v_0 = [U_K : NU_L] = [K^* : NL^*]$ divide il prodotto degli h_n (che è ben definito perché per n sufficientemente grande si ha $h_n = 1$).*

Dimostrazione. Dal corollario precedente abbiamo che $v_0|v_1h_0$; d'altra parte $v_1|v_2h_1$, quindi sostituendo si ha che $v_0|v_2h_1h_0$. Iterando il ragionamento si ha che $\forall n \geq 1 \quad v_0|v_nh_{n-1}\dots h_0$; allora, prendendo n abbastanza grande tale che $v_n = 1$ e $h_{n+1} = 1$ si ha la tesi.

□

Teorema 6.6. *Supponiamo che il gruppo di Galois G sia abeliano. Allora:*

(*a*) *$G_m = G_{m+1}$ se $\varphi(m)$ non è intero;*

(*b*) *$v_n = v_{n+1}h_n \quad \forall n$;*

(*c*) *la mappa canonica $U_K^n/NU_L^n \longrightarrow K^*/NL^*$ è iniettiva.*

Dimostrazione. In generale sappiamo dalla corrispondenza della class field che, se l'estensione è abeliana, $[L : K] = |K^*/NL^*|$.
D'altra parte $[L : K] = |G|$ e:

$$|G| = |G/G_1|\cdot|G_1/G_2|\dots|G_n/G_{n+1}|$$

con n il più piccolo intero tale che $G_{n+1} = \{1\}$. Di conseguenza:

$$v_0 = |K^*/NL^*| = [L : K] = \prod_{m=0}^{\infty} [G_m : G_{m+1}].$$

Inoltre, il corollario 6.5 mostra che $v_0 \mid \prod [G_{\psi(n)} : G_{\psi(n)+1}]$, da cui:

$$\prod_{m\geq 0} [G_m : G_{m+1}] \;\Big|\; \prod_{n\geq 0} [G_{\psi(n)} : G_{\psi(n)+1}]$$

Segue allora che $[G_m : G_{m+1}] = 1$ se m non è della forma $\psi(n)$, cioè se $\varphi(m)$ non è intero, da cui segue la (a).

In modo analogo se per assurdo v_n fosse un divisore proprio di $h_n v_{n+1}$ per qualche intero n, allora v_0 sarebbe un divisore proprio del prodotto degli h_n, cioè di $\prod[G_{\psi(n)} : G_{\psi(n)+1}]$, il che è impossibile per quanto visto al punto precedente. Di conseguenza vale anche la (b).
Infine, usando l'asserzione appena dimostrata e il corollario 6.4 si vede che gli omomorfismi

$$\alpha_n : U_K^{n+1}/NU_L^{\psi(n+1)} \longrightarrow U_K^n/NU_L^{\psi(n)}$$

sono iniettivi $\forall n \geq 0$.
D'altra parte, poiché $U_K/NU_L = K^*/NL^*$, la mappa

$$\beta_n : U_K^n/NU_L^n \longrightarrow K^*/NL^*$$

si ottiene tramite composizione delle $\overline{\alpha}_i$ che sono tutte iniettive; di conseguenza β_n è iniettiva perché composizione di applicazioni iniettive. □

Osservazione 6.7. Osserviamo che la (a) non è altro che il teorema di Hasse-Arf (di cui abbiamo quindi ottenuto un'ulteriore dimostrazione nel caso in cui il campo dei residui $\overline{K}$ sia finito).

Possiamo ora dimostrare due importanti corollari:

Corollario 6.8.
Nelle ipotesi della proposizione precedente, i gruppi $U_K^{n+1}/NU_L^{\psi(n+1)}$ formano una filtrazione decrescente di K^*/NL^*; inoltre si ha che

$$U_K^{n+1}/NU_L^{\psi(n+1)} = 0 \iff G^n = \{1\}.$$

Dimostrazione. Osserviamo che la prima proprietà segue direttamente dal punto (c) della proposizione precedente.
Per quanto riguarda la seconda, notiamo innanzitutto che, dal teorema 6.6, $v_n = 1$ è equivalente a $h_n = h_{n+1} = \ldots = 1$, cioè $G^n = G^{n+1} = \ldots = \{1\}$. Dimostriamo separatamente le due implicazioni:

- $\Rightarrow$ Supponiamo che $U_K^n/NU_L^{\psi(n)} = 0$; allora abbiamo che $v_n = 1$, da cui $v_{n+1} = 1$ e $v_{n+i} = 1 \ \forall i \geq 1$. Per quanto osservato prima si ha anche $h_n = v_n/v_{n+1} = 1$ e, allo stesso modo, $h_{n+i} = 1 \ \forall i \geq 1$.
  Di conseguenza $|G_{\psi(m)}/G_{\psi(m)+1}| \ \ \forall m \geq n$ e quindi $G^n = \{1\}$.

- $\Leftarrow$ Con lo stesso ragionamento precedente, supponiamo $G^n = \{1\}$; allora $h_n = |G_{\psi(n)}/G_{\psi(n)+1}| = 1$ e, $\forall i \geq 1$, $h_{n+i} = 1$.
  Segue quindi che $v_{n+i} = 1 \ \ \forall i \geq 0$, da cui $U_K^n/NU_L^{\psi(n)} = 0$.

□

Corollario 6.9. *Sia c il più grande intero tale che $G_c \neq \{1\}$ e sia $f = \varphi(c)+1$; allora $U_K^f \subset NL^*$, e f il più piccolo intero che soddisfi tale proprietà.*

Dimostrazione. Mostriamo innanzitutto che $U_K^f \subset NL^*$. Dal corollario 2.24 sappiamo che in generale, se $G_{\psi(n+1)} = \{1\}$, $N(U_L^{\psi(n)+1}) = U_K^{n+1}$; vogliamo applicare tale corollario con $n = \varphi(c)$.
Notiamo che per la funzione ψ vale che $\psi(n)+1 \leq \psi(n+1)$; allora, se $n = \varphi(c)$, si ha

$$\psi(\varphi(c)) + 1 = c + 1 \leq \psi(\varphi(c) + 1).$$

Per ipotesi sappiamo che $G_{c+1} = \{1\}$ e quindi anche $G_{\psi(\varphi(c)+1)} \subseteq G_{c+1} = \{1\}$; applicando il corollario otteniamo $U_K^{\varphi(c)+1} = N(U_L^{c+1})$, da cui $U_K^f \subset NL^*$.
Vogliamo ora mostrare che f è il minimo con questa proprietà; dimostriamo quindi che $U_L^{f-1} \not\subset NL^*$.
Notiamo che il punto (c) del teorema precedente ci dice che la mappa canonica ottenuta tramite inclusione e proiezione

$$U_K^n/NU_L^{\psi(n)} \longrightarrow K^*/NL^* \quad \text{è iniettiva;}$$

ciò vuol dire che $U_K^n \cap NL^* = NU_K^{\psi(n)}$.
Supponiamo per assurdo che $U_K^{f-1} \subset NL^*$; allora $U_K^{f-1} \subseteq NU_L^{\psi(f-1)}$ e ciò non è possibile per il corollario precedente (in quanto abbiamo visto che $U_K^n/NU_L^{\psi(n)} = 0 \iff G^n = \{1\}$, e nel nostro caso $G_c = G^{\varphi(c)} = \{1\}$ per ipotesi).

□

Utilizzando tali risultati e le proprietà principali della class field esposte nel capitolo 3 possiamo dare una dimostrazione del teorema 6.1:

Dimostrazione. Sia

$$G = G^{t^1} \supsetneq G^{t^2} \supsetneq \ldots \supsetneq G^{t^m} = \{1\}$$

la successione dei gruppi di ramificazione indicizzati con indici in alto e sia

$$K \subset L_1 \subset L_2 \subset \ldots \subset L_m = L$$

la successione delle sottoestensioni di grado p^i $\forall 1 \leq i \leq m$. Allora per come sono fatti i gruppi di ramificazione di un'estensione di grado p^m si vede che $\forall 1 \leq i \leq m$ $L_i = Fix(G^{t^i+1})$.

Fissiamo $i \in \{1, \ldots, m\}$. Per la corrispondenza di Galois sappiamo che $Gal(L_i/K) \cong G/G^{t^i+1}$. Utilizzando la proposizione 1.51 otteniamo quindi che

$$\forall v \geq 1 \quad (G/G^{t^i+1})^v = G^v G^{t^i+1}/G^{t^i+1} = \begin{cases} G^v/G^{t^i+1} \text{ se } 1 \leq v \leq t^i \\ G^{t^i+1}/G^{t^i+1} = \{1\} \text{ se } v \geq t^i + 1 \end{cases}$$

Di conseguenza l'estensione L_i/K ha come salti della ramificazione esattamente $t^1, \dots t^i$.
Applicando il corollario 6.9 all'estensione L_i/K abbiamo che

$$t^i = \{j \mid U^{j+1} \subset N_{L_i/K}(L_i^*)\}.$$

Per concludere la dimostrazione dobbiamo mostrare che $N_{L_i/K}(L_i^*) = N_{L/K}(L^*)(K^*)^{p^i}$.
Infatti essendo K^{*p^i} un sottogruppo di indice finito di K^*, per la corrispondenza della class field si ha che K^{*p^i} è il sottogruppo normico della massima estensione abeliana F_i di K di esponente p^i. Di conseguenza

$$N(L^*)K^{*p^i} = N(L^*)N(F_i^*) = N(L^* \cap F_i^*).$$

Ma $L \cap F_i$ è la massima sottoestensione di L/K di esponente p^i, cioè esattamente L_i, da cui $N_{L_i/K}(L_i^*) = N_{L/K}(L^*)K^{p^i}$, da cui la tesi.

□

6.3 Il teorema di Marshall e conseguenze

Per i gruppi di ramificazione di un'estensione abeliana di campi completi vale il seguente risultato generale:

Teorema 6.10. *Sia K un campo locale, cioè un campo completo rispetto ad una valutazione discreta e campo dei residui perfetto con $char\overline{K} = p$ (e p eventualmente $= 0$). Indichiamo con $e = e_K$.*
$\forall n \geq 1$ definiamo $f(n) = min\{pn, n+e\}$. Sia L/K un'estensione abeliana finita e sia $G = Gal(L/K)$. Allora la filtrazione dei sottogruppi di ramificazione

$$G \supseteq G^0 \supseteq G^1 \supseteq G^2 \supseteq \dots \supseteq G^r = \{1\}$$

ha le proprietà seguenti:

1. $(G^n)^p \subseteq G^{f(n)}$;

2. *Sia $p_n : G^n/G^{n+1} \to G^{f(n)}/G^{f(n)+1}$ l'applicazione indotta per passaggio al quoziente dal punto precedente.*
   Allora p_n è surgettiva se $n \neq e/(p-1)$.

3. *Se $n = e/(p-1)$ allora coker p_n è isomorfo ad un sottogruppo del gruppo delle radici p-esime dell'unità contenute in K.*

Non riportiamo la dimostrazione di tale risultato in quanto richiede tecniche diverse da quelle usate finora quali la coomologia di gruppi; per i dettagli vedere Marshall [Mar].

Abbiamo precedentemente visto che, se L/K è un'estensione ciclica di grado p^m allora i sottogruppi di ramificazione sono:

- $G^0 = G^1 = \ldots = G^{t^1} = G \cong \mathbb{Z}/p^m\mathbb{Z}$;
- $G^{t^1+1} = \ldots = G^{t^2} = (G)^p \cong p\mathbb{Z}/p^m\mathbb{Z}$;

$\vdots$

- $G^{t^{m-1}+1} = \ldots = G^{t^m} = (G)^{p^{m-1}} \cong p^{m-1}\mathbb{Z}/p^m\mathbb{Z}$;
- $G^{t^m+1} = \ldots = \{1\}$.

In particolare dunque vale che $\forall i \geq 1$ $(G^{t^i})^p = G^{t^{i+1}}$; d'altra parte dal teorema si ha che $(G^{t^i})^p \subseteq G^{f(t^i)}$, e quindi, poiché t^{i+1} è il più grande indice k tale che $G^k = (G^{t^i})^p$, si ha che $t^{i+1} \geq f(t^i)$.
Inoltre sappiamo che l'applicazione $p_n : G^n/G^{n+1} \to G^{f(n)}/G^{f(n)+1}$ è surgettiva se $n \neq e/(p-1)$ e che se $n = e/(p-1)$ allora *coker* p_n è isomorfo ad un sottogruppo delle radici p-esime dell'unità contenute in K.
In particolare, se il campo K non contiene radici p-esime dell'unità, allora *coker* $p_{e/(p-1)} = \{1\}$ e quindi la mappa p_n è surgettiva anche per $n = e/(p-1)$.

Dalla surgettività dell'applicazione p^n segue che, se $n \neq e/(p-1)$ e $f(n)$ è un salto della ramificazione in alto, allora anche n deve essere un salto e, se K non contiene radici p-esime dell'unità ciò accade anche per $n = e/(p-1)$. Più precisamente, se $f(n) = t^{i+1}$ allora necessariamente $n = t^i$.
Sappiamo infatti che se $f(n)$ è un salto allora anche n lo è, e poiché $f(n) > n$ allora $n \in \{t^1, \ldots t^i\}$. Supponiamo per assurdo che $n \leq t^{i-1}$. D'altra parte la funzione f è crescente, quindi:

$$t^{i+1} = f(n) \leq f(t^{i-1}) \leq t^i \text{ per quanto dimostrato prima}$$

e ciò è assurdo perché $t^{i+1} > t^i$.

Abbiamo quindi dimostrato il seguente corollario:

Corollario 6.11. *Se L/K è un'estensione totalmente ramificata ciclica di grado p^m con salti della ramificazione $\{t^1, \ldots, t^m\}$ allora valgono le condizioni seguenti:*

1. *$\forall i \geq 1$ vale $t^{i+1} \geq f(t^i)$;*

2. se $t^{i+1} = f(m)$ *per qualche* $m \neq e/(p-1)$ *allora* $m = t^i$ *e* $t^{i+1} = f(t^i)$.

Inoltre, se K *non contiene radici* p*-esime dell'unità allora la seconda condizione vale anche per* $m = e/(p-1)$.

6.4 Caso $\zeta_p \notin K$

Vogliamo dimostrare la seguente proposizione:

Proposizione 6.12. *Sia* K *un campo completo rispetto ad una valutazione discreta* v_K *con caratteristica* 0 *e campo dei residui finito con caratteristica* p*. Supponiamo inoltre che* K *non contenga radici* p*-esime dell'unità e indichiamo con* $e = v_K(p)$ *e con* $e' = e/(p-1)$*. Sia* L/K *un'estensione totalemente ramificata ciclica di grado* p^m*, con salti della ramificazione* $\{t^1, \dots, t^m\}$*. Valgono allora le seguenti proprietà:*

(a) $1 \leq t^1 < pe'$ *e* $(t^1, p) = 1$*;*

(b) se $t^i < e'$ *allora* $pt^i \leq t^{i+1} < pe'$ *e* $(t^{i+1}, p) = 1$ *se* $t^{i+1} \neq pt^i$*;*

(c) se $t^i \geq e'$ *allora* $t^{i+1} = t^i + e$.

Dimostrazione. Dimostriamo separatamente le tre condizioni.

(a) Supponiamo che t^1 sia un intero e che esista un'estensione K_1/K totalmente ramificata, ciclica di grado p tale che il salto della ramificazione sia proprio t^1 e sia $N = N_{K_1/K}(K_1^*)$ il sottogruppo normico associato all'estensione. Osserviamo innanzitutto che, essendo l'estensione totalmente ramificata, il salto è strettamente maggiore di 0. Sappiamo inoltre dalle proprietà della norma che $(K^*)^p \subset N$, e dal teorema 6.1 che, se t è il salto della ramificazione, $U^t \not\subset N$ e $U^{t+1} \subset N$. Distinguiamo allora due casi:

- Supponiamo $t^1 \geq pe/(p-1)$. Dal corollario 1.7 del primo capitolo sappiamo che, se K non contiene radici p-esime dell'unità allora $U^i \subset (U^{i-e})^p \ \forall i \geq pe/(p-1)$. Applicando ciò al nostro caso abbiamo quindi che
$$U^{t^1} \subset (U^{t^i - e})^p \subset (K^*)^p \subset N$$
e ciò è assurdo per quanto appena visto.

– Supponiamo $1 \leq t^1 < pe/(p-1)$ e $p \mid t^1$. Allora $t^1 = ph$, quindi

$$U^{t^1} = U^{ph} \subset (U^h)^p \subset (K^*)^p \subset N$$

e ciò è assurdo per lo stesso ragionamento precedente.

Per il salto t^1 valgono quindi le condizioni seguenti:

$$1 \leq t^1 < pe/(p-1) \quad \text{e} \quad (t^1, p) = 1.$$

(b) Supponiamo $t^i < e'$; allora $f(t^i) = min\{pt^i, t^i + e\} = pt^i$.

1. Supponiamo per assurdo che $t^{i+1} \geq pe = e + e'$. Allora

$$t^{i+1} = f(m) \quad con \quad m = t^{i+1} - e \geq e' > t^i$$

e ciò è assurdo per il corollario 6.11.
Abbiamo quindi che:

$$pt^i \leq t^{i+1} < pe'.$$

2. Supponiamo per assurdo che t^{i+1} sia tale che $pt^i < t^{i+1} < pe'$ e $t^{i+1} \equiv 0 \ (p)$. Allora $t^{i+1} = pm = f(m)$ con $m > t^i$ e ciò è assurdo sempre per il corollario 6.11.
In questo caso allora la condizione è verificata.

(c) Supponiamo infine $t^i \geq e'$; allora $f(t^i) = min\{pt^i, t^i + e\} = t^i + e$. Abbiamo visto che in generale $t^{i+1} \geq f(t^i) = t^i + e$.
Supponiamo allora per assurdo che $t^{i+1} > t^i + e$. Si ha quindi

$$t^{i+1} = f(m) \quad con \quad m = t^{i+1} - e > t^i$$

e ciò è ancora assurdo per il corollario 6.11.
In questo caso abbiamo quindi che $t^{i+1} = t^i + e$.

□

6.5 Caso $\zeta_p \in K$

Utilizzando ancora in corollario 6.11 vogliamo dimostrare l'analoga proposizione per il caso $\zeta_p \in K$:

Proposizione 6.13. *Sia K un campo completo rispetto ad una valutazione discreta v_K con caratteristica 0 e campo dei residui finito con caratteristica p. Supponiamo inoltre che K contenga almeno una radice p-esima dell'unità non banale; indichiamo con $e = v_K(p)$ e con $e' = e/(p-1)$. Sia L/K un'estensione totalemente ramificata ciclica di grado p^m, con salti della ramificazione $\{t^1, \ldots, t^m\}$. Valgono allora le seguenti proprietà:*

(a) $1 \leq t^1 \leq pe'$ *e* $(t^1, p) = 1$ *se* $t^1 \neq pe'$*;*

(b) se $t^i < e'$ *allora* $pt^i \leq t^{i+1} < pe'$ *e* $(t^{i+1}, p) = 1$ *se* $t^{i+1} \neq pt^i$ *e* $t^{i+1} \neq pe'$*;*

(c) se $t^i \geq e'$ *allora* $t^{i+1} = t^i + e$*.*

Dimostrazione. Anche in questo caso dimostriamo separatamente. Osserviamo che la dimostrazione è analoga al caso in cui $\zeta_p \notin K$, e le differenze dipendono dal fatto che, nel caso in cui $\zeta_p \in K$ vale che $U_K^{pe/(p-1)} \notin K^{*p}$.

(a) La condizione su t^1 segue in modo diretto dall'analisi delle estensioni di grado p del capitolo 4 e in particolare dal corollario 4.8.

(b) Supponiamo $t^i < e'$; allora $f(t^i) = min\{pt^i, t^i + e\} = pt^i$.

1. Supponiamo per assurdo che $t^{i+1} > pe' = e + e'$. Allora
$$t^{i+1} = f(m) \quad con \quad m = t^{i+1} - e > e' \geq t^i$$
per l'ipotesi induttiva e ciò è assurdo per il corollario 6.11.
Abbiamo quindi che:
$$pt^i \leq t^{i+1} \leq pe'.$$
2. Supponiamo per assurdo che t^{i+1} sia tale che $pt^i < t^{i+1} < pe'$ e $t^{i+1} \equiv 0\ (p)$. Allora $t^{i+1} = pm = f(m)$ con $m > t^i$ e ciò è assurdo sempre per il corollario 6.11. In questo caso allora la condizione è verificata.

(c) Supponiamo ora $t^i \geq e'$; allora $f(t^i) = min\{pt^i, t^i + e\} = t^i + e$. Abbiamo visto che in generale vale che $t^{i+1} \geq f(t^i) = t^i + e$.
Supponiamo allora per assurdo che $t^{i+1} > t^i + e$. Si ha quindi
$$t^{i+1} = f(m) \quad con \quad m = t^{i+1} - e > t^i$$
e ciò è ancora assurdo per il corollario 6.11.
In questo caso abbiamo quindi che $t^{i+1} = t^i + e$.

□

Per ultimare la dimostrazione delle condizioni necessarie ci resta da dimostrare la seguente proposizione:

Proposizione 6.14. *Sia K un campo completo rispetto ad una valutazione discreta v_K che soddisfi le condizioni del teorema di Miki. Supponiamo che esista L/K estensione ciclica totalmente ramificata di grado p^m con salti della ramificazione $\{t^1, \ldots, t^m\}$. Indichiamo con n (se esiste) il più piccolo intero tale che $t^n \geq e'$. Allora:*

1. *Se $\overline{K} = \mathbb{F}_p$ ed esiste $1 \leq j \leq m$ tale che vale la condizione $C(j)$ del teorema di Miki, allora $j \geq n - s + 1$ e $m \leq j + s - 1$.*

2. *Se $\overline{K} \neq \mathbb{F}_p$ ed esiste $1 \leq I \leq m$ tale che*

$$t^I = \lambda_l = pe', \ t^{I-1} < e' \ e \ t^{I-i} < \lambda_{l-i} \ \forall i \in \{1, 2 \ldots, l\},$$

allora $I = n$ e $m \leq I + s - 1$.

Tale questione è direttamente legata alla presenza delle radici p-esime dell'unità nei sottogruppi normici associati all'estensione L/K.

$\forall i \geq 1$ sia $\mathcal{F}_i$ la famiglia di tutti i sottogruppi N di K^* associati, tramite la corrispondenza della class field, ad estensioni cicliche totalmente ramificate di grado p^i con salti della ramificazione $\{t^1, \ldots, t^i\}$. Denotiamo con

$$S(t^1 \ldots t^i) = S_i = \bigcup_{N \in \mathcal{F}_i} N \quad \forall 0 \leq i \leq n.$$

Vale allora il seguente lemma:

Lemma 6.15. *Nelle ipotesi della proposizione precedenti valgono le seguenti affermazioni:*

- *Se $\overline{K} = \mathbb{F}_p$ e vale la condizione $C(j)$ per qualche $1 \leq j \leq m$, allora $\zeta_s \in S_{j-1} - S_j$.*

- *Se $\overline{K} \neq \mathbb{F}_p$ ed esiste $1 \leq I \leq m$ tale che*

$$t^I = \lambda_l = pe', \ t^{I-1} < e' \ e \ t^{I-i} < \lambda_{l-i} \ \forall i \in \{1, 2 \ldots, l\},$$

allora $\zeta_s \in S_{I-1} - S_I$.

Osservazione 6.16. Notiamo che per dimostrare che $\zeta_s \in S_{j-1}$ basta costruire un sottogruppo normico N di K^* associato ad un'estensione ciclica totalmente ramificata di grado p^{j-1} con salti della ramificazione $\{t^1, \ldots, t^{j-1}\}$ e tale che $\zeta_s \in N$, e tale costruzione sarà resa esplicita nella dimostrazione della sufficienza delle condizioni nel prossimo capitolo.
La dimostrazione del fatto che $\zeta_s \notin S_j$ invece richiede un altro tipo di calcoli. Per i dettagli su tale dimostrazione si veda [Mik1].

Per dimostrare la proposizione 6.14 abbiamo bisogno di un altro lemma.

6.6 Immersioni di estensioni cicliche

Sia K un campo completo rispetto ad una valutazione discreta v_K. Supponiamo $charK = 0$, $char\overline{K} = p$ e che il campo dei residui $\overline{K}$ sia perfetto (non necessariamente finito). Supponiamo in aggiunta che K contenga le radici p-esime dell'unità. Vogliamo dimostrare il seguente teorema:

Teorema 6.17. *Un'estensione ciclica L/K di grado p^n può essere immersa in un'estensione ciclica di di grado p^{n+1} se e solo se le radici p-esime dell'unità contenute in K^* sono norme di elementi di L.*

Dimostrazione.

$\Rightarrow$ Sia L/K un'estensione ciclica di grado p^n e supponiamo che esista M/K estensione ciclica di grado p^{n+1} che contenga L/K. Utilizzando la teoria di Kummer sappiamo che esiste $a \in L^*$ tale che $M = L(b)$ con $b^p = a$.

$$\begin{array}{c} M = L(\sqrt[p]{a}) \\ \Big| \; p \\ L \\ \Big| \; p^n \\ K \end{array}$$

Poiché L/K è un'estensione di Galois allora $\forall g \in Gal(L/K)$ esiste un elemento $x_g \in K^*$ tale che $g(a) = ax_g^p$. Sia infatti $h \in Gal(M/K)$ tale che $h_{|_L} = g$ e sia $x_g = h(b)/b$; allora:

$$g(a) = h(a) = h(b^p) = (h(b))^p = b^p \; x_g^p = a \; x_g^p.$$

Mostriamo ora che $x_g \in K$ e per fare ciò mostriamo per prima cosa che x_g è lasciato fisso da tutti gli elementi di $Gal(M/L)$. $\forall f \in Gal(M/L)$ si ha che $f(b) = \zeta b$ per qualche ζ tale che $\zeta^p = 1$. Di conseguenza

$$f(h(b)/b) = f(h(b))/f(b);$$

ma $f \in Gal(M/L) \subset Gal(M/K)$, $h \in Gal(M/K)$ e tale gruppo è commutativo, quindi

$$f(h(b))/f(b) = h(f(b))/f(b) = h(\zeta b)/\zeta b = h(\zeta)h(b)/\zeta b = h(b)/b.$$

Si ha quindi che $h(b)/b \in L^*$.
Sia allora g un generatore di $Gal(L/K)$ e mostriamo che l'elemento x_g

definito prima è tale che $N_{L/K}(x_g) = \zeta$.
Osserviamo innanzitutto che, poiché $x_g^p = g(a)/a$, si ha

$$(N_{L/K}(x))^p = N_{L/K}(x^p) = N_{L/K}(g(a)/a) = N_{L/K}(g(a))/N_{L/K}(a) = 1.$$

Basta quindi dimostrare che $N_{L/K}(x) \neq 1$.
Supponiamo per assurdo che $N_{L/K}(x) = 1$. Poiché L/K è ciclica per ipotesi, applicando il teorema 90 di Hilbert esiste un elemento $y \in L^*$ tale che $x = g(y)/y$. Vale quindi che

$$g(a)/a = x^p = g(y^p)/y^p,$$

da cui $g(a/y^p) = a/y^p$, cioè $a/y^p \in K^*$. D'altra parte, se $\overline{\alpha}$ è un elemento tale che $\overline{\alpha}^p = a$, si ha

$$M = L(\alpha/y) = LM' \text{ con } M' = K(\alpha/y).$$

Poiché $M' \cap L = K$ segue che $Gal(M/K) \cong \mathbb{Z}/p\mathbb{Z} \times Gal(M'/K)$, il che è assurdo perché per ipotesi $Gal(M/K)$ è ciclico.

$\Leftarrow$ Sia L/K un'estensione ciclica di grado p^n e supponiamo che esista $x \in L^*$ tale che $N_{L/K}(x) = \zeta$. Vale allora $N_{L/K}(x^p) = (N_{L/K}(x))^p = 1$, quindi usando il teorema 90 di Hilbert esiste $a \in L^*$ tale che $x^p = g(a)/a$. Vogliamo mostrare che, presa α tale che $\alpha^p = a$, l'estensione $L(\alpha)/K$ è ciclica di ordine p^{n+1} su K.
Sia allora b tale che $b^p = a$, e poniamo $M = K(b)$. Osserviamo che $b \notin K^*$ in quanto se per assurdo $b \in K^*$ allora

$$x = (g(b)/b)\zeta^n$$

per qualche n e quindi $N_{L/K}(x) = 1$. Si ha allora che $[M : K] = p^{n+1}$. Per dimostrare che l'estensione è ciclica consideriamo l'automorfismo h di M/K definito da $h(b) = bx$ e dimostriamo che tale h ha ordine p^{n+1}. Osserviamo innanzitutto che $h_{|_L} = g$; infatti:

$$h(a) = h(b^p) = (h(b))^p = (bx)^p = b^p x^p = a(g(a)/a) = g(a).$$

Calcoliamo allora $h^{p^n}(b)$:

$$h^{p^n}(b) = h^{p^n-1}(bx) = \ldots = b\prod_{i=0}^{p^n-1} g^i(x) = bN_{L/K}(x) = b\zeta \neq b.$$

L'ordine di h è quindi necessariamente p^{n+1}; di conseguenza M/K è un'estensione di Galois e $Gal(M/K) \cong \mathbb{Z}/p^{n+1}\mathbb{Z}$. □

Possiamo finalmente dimostrare la proposizione 6.14.

Dimostrazione.

1. Supponiamo $\overline{K} = \mathbb{F}_p$; sia M/K un'estensione ciclica totalmente ramificata di grado p^m con salti in alto della ramificazione $\{t^1, \dots, t^m\}$ e supponiamo che esista $1 \leq j \leq m$ tale che valga la condizione $C(j)$.
   Dal lemma 6.15 ciò implica che $\zeta_s \in S_{j-1} - S_j$.

   - Mostriamo che $m \leq j + s - 1$.
     Supponiamo per assurdo che $m \geq j+s$ e sia L/K la sottoestensione di M/K di grado p^{j+s}; allora L/K è un'estensione ciclica totamente ramificata con salti in alto della ramificazione $\{t^1, \dots, t^{j+s}\}$.
     $\forall 1 \leq i \leq j + s - 1$ denotiamo con L_i la sottoestensione di L di grado p^i; allora, per il teorema 6.17 vale $\zeta_1 \in N_{L_{j+s-1}/K}({L_{j+s-1}}^*)$ in quanto L_{j+s-1} è un'estensione ciclica di grado p^{j+s-1} immersa in un'estensione di grado p^{j+s}.
     Tuttavia $\zeta_1 = \zeta_s^{p^{s-1}}$ quindi, utilizzando il corollario 3.21, si ha che $\zeta_s^{p^{s-2}} \in N_{L_{j+s-2}/K}({L_{j+s-2}}^*)$.
     Iterando il ragionamento otteniamo quindi che $\zeta_s \in N_{L_j/K}(L_j^*)$; ciò vuol dire che esiste un'estensione L_j/K ciclica totalmente ramificata di grado p^j con salti in alto della ramificazione $\{t^1, \dots, t^j\}$ tale che ζ_s appartiene al sottogruppo normico associato, il che è assurdo perché $\zeta_s \notin S_j$.

   - Mostriamo che, se esiste $1 \leq n \leq m$ tale che $t^n \geq e'$, allora si ha $j \geq n + s - 1$.
     Supponiamo per assurdo $j \leq n - s$ e sia L/K la sottoestensione di M/K di grado $j + s - 1$, che è ben definita in quanto

     $$j + s - 1 \leq n - s + s - 1 \leq n - 1 \leq m - 1.$$

     Allora L/K è un'estensione ciclica totalmente ramificata di grado p^{j+s-1} con salti in alto della ramificazione $\{t^1, \dots, t^{j+s-1}\}$. Notiamo ora che, se $j \leq n-s$, allora $j+s-1 \leq n-1$; di conseguenza per ipotesi l'ultimo salto della ramificazione di L/K è $t^{j+s-1} < e'$. Applicando $\psi = \psi_{L/K}$ ad ambo i menbri otteniamo quindi che $\psi(t^{j+s-1}) < \psi(e')$, e dunque, se indichiamo con G_i l'i-esimo gruppo di ramificazione di L/K, allora

     $$G_{\psi(e')} \subseteq G_{\psi(t^{j+s-1})} = \{1\}.$$

     Utilizzando il corollario 2.24 abbiamo che, se $G_{\psi(h)} = \{1\}$, allora $N_{L/K}(U_L^{\psi(h)}) = U_K^h$. Essendo nel nostro caso $G_{\psi(e')} = \{1\}$, si ha

$N_{L/K}(U_L^{\psi(e')}) = U_K^{e'}$ e quindi, poiché $v_K(\zeta_1 - 1) = e'$, esiste $x \in U_L^{\psi(e')}$ tale che $N_{L/K}(x) = \zeta_1 = \zeta_s^{p^{s-1}}$.
Utilizzando nuovamente il corollario 3.21 abbiamo che, indicando con L_i la sottoestensione di L di grado p^i $\forall 1 \leq i \leq j+s-1$, allora $\zeta_s^{p^{s-2}} \in N_{L_{j+s-2}/K}(L_{j+s-2}^*)$ e quindi iterando il ragionamento anche $\zeta_s \in N_{L_j/K}(L_j^*)$, il che è assurdo in quanto $\zeta_s \notin S_j$. Di conseguenza necessariamente $j \geq n - s + 1$.

2. Supponiamo $\overline{K} \neq \mathbb{F}_p$ e che esista $1 \leq I \leq m$ tale che

$$t^I = \lambda_l = pe', \ t^{I-1} < e' \text{ e } t^{I-i} < \lambda_{l-i} \ \forall i \in \{1, 2 \ldots, l\}.$$

Si vede che allora banalmente che $I = n$; infatti $t^{I-1} < e'$ e $t^I = pe'$, quindi I è proprio il più piccolo intero tale che $t^I \geq e'$, cioè $I = n$. Per il lemma 6.15 ciò significa che $\zeta_s \in S_{n-1} - S_n$. Con la stessa dimostrazione del punto precedente si ha quindi che $m \leq n + s - 1$, da cui la tesi.

□

Capitolo 7

Condizioni sufficienti

In tale capitolo vogliamo dare una dimostrazione del fatto che le condizioni date dal teorema di Miki sono sufficienti. Per fare ciò daremo nei vari casi una costruzione esplicita del sottogruppo normico associato ad un'estensione ciclica e totalmente ramificata di grado p^m tramite la corrispondenza della class field in modo che i salti della ramificazione siano esattamente $\{t^1, \dots, t^m\}$. Per imporre le condizioni sui salti in alto della ramificazione dell'estensione in termini del sottogruppo normico associato ricordiamo l'enunciato del teorema 6.1 dimostrato nel capitolo precedente:

Teorema. *Sia K un campo completo rispetto ad una valutazione discreta con $charK = 0$ e campo dei residui finito di caratteristica p. Sia L/K un'estensione ciclica totalmente ramificata di grado p^m . Indichiamo con $t^1, \dots t^m$ i salti in alto dell'estensione L/K.*
Allora vale:

$$t^i = min\{j \in \mathbb{N} \mid U^{(j+1)} \subseteq N_{L/K}(L^*)K^{*p^i}\} \qquad \forall i = 1, \dots m.$$

7.1 Costruzione nel caso $\zeta_p \notin K$

Sia K un campo completo rispetto ad una valutazione discreta v_K con $charK = 0$ e campo dei residui finito di caratteristica p. Supponiamo che $\zeta_p \notin K$ e denotiamo con $e = v_K(p)$, $e' = e/(p-1)$ (che in questo caso non è necessariamente intero).
Fissiamo una m-pla di interi $\{t^1, \dots, t^m\}$ che soddisfi le condizioni della formulazione equivalente del teorema di Maus 5.2, cioè:

- $1 \leq t^1 < e'p$ e $(t^1, p) = 1$;

- se $t^i < e'$ allora t^{i+1} soddisfa una delle due condizioni seguenti:
  - $t^{i+1} = pt^i$;
  - $pt^i < t^{i+1} < pe/(p-1)$ e $(p, t^{i+1}) = 1$;
- se $t^i \geq e'$; allora $t^{i+1} = t^i + e$.

Vogliamo costruire un opportuno sottogruppo N di K^* in modo che l'estensione ad esso associata tramite la class field abbia esattamente i salti cercati. Per fare ciò distinguiamo due casi distinti, cioè il caso in cui $\overline{K} = \mathbb{F}_p$ e il caso in cui $\overline{K} \neq \mathbb{F}_p$.

7.1.1 Caso $\overline{K} = \mathbb{F}_p$

Supponiamo che il grado di inerzia del campo K sia $f = 1$, cioè che il campo dei residui sia $\overline{K} = \mathbb{F}_p$.

Fissiamo $\{t^1, \ldots, t^m\}$ una m-pla di interi che soddisfi le proprietà precedenti. Denotiamo con J il seguente insieme:

$$J = \{t_{(1)}, \ldots, t_{(r)}\} = \{t^1, \ldots, t^m\} - \{f(t^i) \mid i = 1, \ldots, m\}.$$

Chiamiamo inoltre $I = \{1 \leq x < pe' \mid (x, p) = 1\}$.

Dal corollario 1.10 sappiamo che, nel caso in cui il campo K non contenga radici p-esime dell'unità, detto π un uniformizzante di K, una base di U^1 con $\mathbb{Z}_p$-modulo è dato da elementi della forma

$$\{\eta_x\}_{x \in I} \quad \text{con} \quad \eta_x = 1 + \pi^x.$$

Notiamo che, per le condizioni sull'insieme $\{t^1, \ldots, t^m\}$, $t^1 \in I \cap J$; di conseguenza $I \cap J \neq \varnothing$.
Chiamiamo inoltre $\eta_{(z)} = \eta_{t(z)}$ e, $\forall z = 1, \ldots, r$, indichiamo con i_z l'indice per cui $t^i = t_{(z)}$. Ovviamente, poiché $t^1 = t_{(1)}$, si ha che $i_1 = 1$.
Definiamo inoltre, $\forall z = 2, \ldots, r$, l'elemento ε_z nel modo seguente:

$$\varepsilon_z = \eta_{(1)}^{-p^{i_z - 1}} \eta_{(z)}.$$

Consideriamo allora il sottogruppo N di K^* definito nel modo seguente:

$$N = < K^{*p^m},\ \pi,\ \eta_x \text{ con } x \in I - J,\ \varepsilon_z \text{ se } z = 2, \ldots, r > .$$

Vogliamo dimostrare che l'estensione L/K associata al sottogruppo N utilizzando la corrispondenza della class field è ciclica, totalmente ramificata di grado p^m e che ha come salti dell'estensione proprio $\{t^1, \ldots, t^m\}$.

- Osserviamo innanzitutto che l'estensione L/K è totalmente ramificata in quanto $\pi \in N$.

- Dimostriamo che K^*/N è un gruppo ciclico di ordine p^m e precisamente generato da $\eta_{(1)}N$.
  Infatti osserviamo innanzitutto che le classi $N, \eta_{(1)}N, \eta_{(1)}^2N, \ldots, \eta_{(1)}^{p^m-1}N$ sono tutte distinte in quanto nessuna delle potenze $\eta_{(1)}^i$ con $i \leq p^m - 1$ appartiene al sottogruppo N.
  Per mostrare che questi sono gli unici elementi di K^*/N mostriamo che tutti gli altri generatori di U^1 diversi da $\eta_{(1)}$ appartengono ad una delle classi di equivalenza descritte sopra (ciò basta in quanto $K^* =< \pi > \times \mathbb{F}_p^* \times U^1$ e sia $< \pi >$ che $\mathbb{F}_p^*$ sono contenuti in N).
  Distinguiamo dunque due casi:

  - Se η_x è tale che $x \in I - J$, allora $\eta_x \in N$ per costruzione.
  - Se invece η_x è tale che $x \in J$ e $x \neq t^1$, allora esiste $z \in \{2, \ldots, r\}$ tale che $\eta_x = \eta_{(z)}$. Di conseguenza:

    $$\eta_{(z)} = \eta_{(1)}^{p^{i_z-1}} \varepsilon_z \in \eta_{(1)}^{p^{i_z-1}} N$$

    e banalmente $i_z \leq m$ quindi $\eta_{(1)}^{p^{i_z-1}} N$ è una delle classi elencate sopra.

  Di conseguenza K^*/N è ciclico di ordine p^m. D'altra parte, dal teorema 3.3 del capitolo 3 si ha che il gruppo di Galois dell'estensione abeliana finita associata ad N è isomorfo a K^*/N, quindi nel nostro caso l'estensione L/K associata ad N è ciclica di grado p^m come voluto.

Dimostriamo ora che i salti della ramificazione dell'estensione L/K sono esattamente $t^1, \ldots, t^m$.

$\forall 1 \leq i \leq m$ indichiamo con $N_i = NK^{*p^i}$. Per il teorema 6.1 basta quindi dimostrare che $\forall i \in \{1, \ldots, m\}$ vale $U^{t^i} \not\subset N_i$ e $U^{t^i+1} \subset N_i$.

- Sia u il maggior elemento di $\{1, \ldots, r\}$ tale che $t_{(u)} \leq t^i$.
  Dalla definizione dell'insieme J si ha che $t^i = f(t^{i-1}) = \ldots = f^{i-i_u}(t_{(u)})$.
  Consideriamo allora l'elemento $\eta_{(u)}$; abbiamo quindi che:

  $$\eta_{(u)} = \begin{cases} \eta_{(1)} \in N_0 - N_1 = N_{i_1-1} - N_{i_1} & \text{se } u = 1 \\ \\ \eta_{(1)}^{p^{i_u-1}} \varepsilon_u \in N_{i_u-1} - N_{i_u} & \text{se } u \geq 2 \end{cases}$$

  Di conseguenza:

– se $u = 1$ allora $\eta_{(1)}^{p^{i-i_1}} = \eta_{(1)}^{p^{i-1}} \in N_{i-1} - N_i$;
– se $u \geq 2$

$$\eta_{(u)}^{p^{i-i_u}} = \varepsilon_u^{p^{i-i_u}} (\eta_{(1)}^{p^{i_u-1}})^{p^{i-i_u}} = \eta_{(1)}^{p^{i-1}} \varepsilon_u^{p^{i-i_u}} \in N_{i-1} - N_i.$$

Abbiamo quindi in ogni caso che $\eta_{(u)}^{p^{i-i_u}} \in N_{i-1} - N_i$.
D'altra parte

$$v_K(\eta_{(u)}^{p^{i-i_u}} - 1 \geq f^{i-i_u}(v_K(\eta_{(u)} - 1)) = f^{i-i_u}(t_{(u)}) = t^i,$$

quindi $\eta_{(u)}^{p^{i-i_u}} \in U^{t^i}$ ma $\eta_{(u)}^{p^{i-i_u}} \notin N_i$, come voluto.

- Mostriamo ora che $U^{t^i+1} \subset N_i$.
$\forall x \geq t^i + 1$ indichiamo con n_x il più piccolo intero tale che $x = f^{n_x}(v_x)$ e $v_x \in I$. Osserviamo che U^{t^i+1} è generato come $\mathbb{Z}_p$-modulo dagli elementi della forma $\{\eta_{v_x}^{p^{n_x}}\}_{x \geq t^i+1}$; mostriamo allora che ognuno di tali elementi appartiene a N_i. Distinguiamo due casi:

  – se $v_x \neq t_{(z)} \quad \forall z \in \{1, \ldots, r\}$ allora si ha per costruzione che $\eta_{v_x} \in N$ e quindi anche $\eta_{v_x}^{p^{n_x}} \in N \subset N_i$;
  – supponiamo che esista $z \in \{1, \ldots, r\}$ tale che $v_x = t_{(z)}$. Abbiamo quindi che:

$$\eta_{v_x} = \eta_{(z)} = \begin{cases} \eta_{(1)} \in N_0 = N_{i_1-1} & \text{se } z = 1 \\ \eta_{(1)}^{p^{i_z-1}} \varepsilon_z \in N_{i_z-1} & \text{se } z \geq 2 \end{cases}$$

  Di conseguenza:
    * se $z = 1$ allora $\eta_{v_x}^{p^{n_x}} = \eta_{(1)}^{p^{n_x}} \in N_{n_x} = N_{n_x+i_1-1}$;
    * se $z \geq 2$ allora

$$\eta_{v_x}^{p^{n_x}} = (\eta_{(1)}^{p^{i_z-1}} \varepsilon_z)^{p^{n_x}} = \eta_{(1)}^{p^{+n_x+i_z-1}} \varepsilon_z^{p^{n_x}} \in N_{n_x+i_z-1}.$$

  In entrambi i casi vale che $\eta_{v_x}^{p^{n_x}} \in N_{n_x+i_z-1}$.
  Vogliamo ora dimostrare che $N_{n_x+i_z-1} \subset N_i$; distinguiamo allora due casi:
    * se $i_z + n_x \geq m + 1$, allora banalmente $i_z + n_x \geq i + 1$, da cui $i_z + n_x - 1 \geq i$;
    * se $i_z + n_x \leq m$, allora $t^i + 1 \leq f^{n_x}(t_{(z)}) \leq t^{i_z+n_x}$, da cui si ha $i + 1 \leq i_z + n_x$, cioè $i_z + n_x - 1 \geq i$.

  Poiché $i_z + n_x - 1 \geq i$ allora $N_{n_x+i_z-1} \subset N_i$ e quindi la tesi.

7.1.2 Caso generale

Supponiamo ora che il grado di inerzia di K sia $\mathfrak{f} > 1$. In questo caso allora il campo dei residui sarà $\overline{K} = \mathbb{F}_q$ con $q = p^{\mathfrak{f}}$ e sappiamo che $\overline{K}$ è uno spazio vettoriale su $\mathbb{F}_p$ di dimensione $\mathfrak{f}$.
Fissiamo $\{t^1, \dots, t^m\}$ una m-pla di interi che soddisfi le proprietà precedenti. Come nel caso precedente indichiamo con J il seguente insieme:

$$J = \{t_{(1)}, \dots, t_{(r)}\} = \{t^1, \dots, t^m\} - \{f(t^i) \mid i = 1, \dots, m\}.$$

e con $I = \{x \in \mathbb{Z} \mid 1 \leq x < pe' \text{ e } (p, x) = 1\}$.

Siano $a_1, \dots a_{\mathfrak{f}}$ degli elementi di K tali che $\overline{a}_1, \dots \overline{a}_{\mathfrak{f}}$ siano una base di $\overline{K}$ come spazio vettoriale su $\mathbb{F}_p$. Definiamo inoltre l'insieme

$$F = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x \in I,\ 1 < y < f\}.$$

Allora, se indichiamo con $\eta_{(x,y)} = 1 + a_y \pi^x$, dove π è un uniformizzante di $\overline{K}$, l'insieme $\{\eta_{(x,y)}\}_{(x,y)\in F}$ costituisce una base di U^1 come $\mathbb{Z}_p$-modulo.
Definiamo ora l'insieme $F_1 = \{(t_{(z)}, 1) \mid 1 \leq z \leq r\}$. Inoltre, $\forall z \in \{1, \dots, r\}$, poniamo

$$\eta_{(z)} = \eta_{(t_{(z)},1)} \quad \text{e} \quad \varepsilon_z = \eta_{(1)}^{-p^{i_z - 1}} \eta_{(z)}.$$

Consideriamo allora il sottogruppo N di K^* definito nel modo seguente:

$$N = < K^{*p^m},\ \pi,\ \eta_{(x,y)} \text{ con } x \in F - F_1,\ \varepsilon_z \text{ se } z = 2, \dots, r > .$$

Utilizzando gli stessi ragionamenti del caso precedente dimostriamo che l'estensione L/K associata al sottogruppo N utilizzando la corrispondenza della class field è ciclica, totalmente ramificata di grado p^m e che ha come salti dell'estensione proprio $\{t^1, \dots, t^m\}$. Infatti:

- Poiché $\pi \in N$ l'estensione associata ad N è totalmente ramificata.

- Il gruppo K^*/N è ciclico di ordine p^m ed è generato dall'elemento $\eta_{(1)}N$. Infatti osserviamo che anche in questo caso le classi N, $\eta_{(1)}N$, $\eta_{(1)}^2 N$, $\dots$, $\eta_{(1)}^{p^m-1} N$ sono tutte distinte in quanto nessuna delle potenze $\eta_{(1)}^i$ con $i \leq p^m - 1$ appartiene al sottogruppo N.
  Per mostrare che non ce ne sono altre facciamo vedere che ognuno dei generatori di U^1 diverso da $\eta_{(1)}$ è in una delle classi elencate sopra. Consideriamo allora $\eta_{(x,y)}$ e distinguiamo due casi:

  - se $(x, y) \in F - F_1$ allora $\eta_{(x,y)} \in N$ per costruzione;

– supponiamo $(x,y) \in F_1$; allora $y = 1$ ed esiste $z \in \{2,\dots r\}$ tale che $\eta_{(x,y)} = \eta_{(z)}$. In questo caso allora

$$\eta_{(x,y)} = \eta_{(z)} = \eta_{(1)}^{p^{i_z-1}} \varepsilon_z \in \eta_{(1)}^{p^{i_z-1}} N$$

ed essendo banalmente $i_z \leq m$ si ha che $\eta_{(1)}^{p^{i_z-1}} N$ è una delle classi descritte sopra.

Di conseguenza K^*/N è un gruppo ciclico di grado p^m e l'estensione associata ad N è ciclica di grado p^m per le proprietà della teoria della class field.

Mostriamo ora che che i salti della ramificazione dell'estensione L/K sono esattamente $t^1,\dots,t^m$.

Come nel caso precedente $\forall 1 \leq i \leq m$ chiamiamo $N_i = NK^{*p^i}$. Per il teorema 6.1 basta quindi dimostrare che $\forall i \in \{1,\dots,m\}$ si ha $U^{t^i} \not\subset N_i$ e $U^{t^i+1} \subset N_i$.

La dimostrazione della proprietà $U^{t^i} \not\subset N_i$ è identica a quella nel caso in cui $\overline{K} = \mathbb{F}_p$ (anche qui basta prendere u il maggior elemento di $\{1,\dots,r\}$ tale che $t_{(u)} \leq t_i$ e si dimostra allo stesso modo che $\eta_{(u)}^{p^{i-i_u}}$ è un elemento di U^{t^i} che non appartiene ad N_i).
Dimostriamo allora che $U^{t^i+1} \subset N_i$.
Come prima $\forall x \geq t^i + 1$ sia n_x il più piccolo intero tale che $x = f^{n_x}(v_x)$ con $v_x \in I$. Notiamo allora che in questo caso U^{t^i+1} è generato dagli elementi della forma $\{\eta_{(v_x,y)}^{p^{n_x}}\}$ con $x \geq t^i + 1$ e $y \in \{1,\dots,f\}$. Vogliamo mostrare che gli elementi di questa forma appartengono a N_i. Distinguiamo allora due casi:

- supponiamo che $v_x \neq t_{(z)} \quad \forall z \in \{1,\dots,r\}$; allora si ha per costruzione che $\eta_{(v_x,y)} \in N \ \forall y \in \{1,\dots,f\}$ e quindi anche $\eta_{v_x}^{p^{n_x}} \in N \subset N_i$;
- supponiamo che esista $z \in \{1,\dots,r\}$ tale che $v_x = t_{(z)}$. Allora:
  – gli elementi del tipo $\eta_{(t_{(z)},y)}$ con $y \geq 2$ appartengono ad N per costruzione. In questo caso quindi
  $$\eta_{(t_{(z)},y)}^{p^{n_x}} \in N \subset N_i.$$
  – gli elementi del tipo $\eta_{(t_{(z)},1)}$ sono proprio quelli della forma $\eta_{(z)}$. Allora come nella dimostrazione precedente
  $$\eta_{(v_x,1)} = \eta_{(z)} = \begin{cases} \eta_{(1)} \in N_0 = N_{i_1-1} & \text{se } z = 1 \\ \eta_{(1)}^{p^{i_z-1}} \varepsilon_z \in N_{i_z-1} & \text{se } z \geq 2 \end{cases}$$

da cui quindi $\eta_{(v_x,1)}^{p^{n_x}} \in N_{n_x+i_z-1}$. Con lo stesso ragionamento del caso precedente si ha che $i_z + n_x \geq i+1$ e quindi $N_{n_x+i_z-1} \subset N_i$.

Di conseguenza $U^{t^i+1} \subset N_i$, da cui segue la tesi.

7.2 Costruzione nel caso $\zeta_p \in K$

Analizziamo ora il caso in cui $\zeta_p \in K$.
Sia K un campo con $char(K) = 0$ e $\overline{K}$ campo dei residui finito di caratteristica p. Sia $e = v_K(p)$ e sia $e' = e/(p-1)$. Indichiamo con ζ_i una radice p^i-esima dell'unità tali che $\zeta_{i+1}^p = \zeta_i \ \forall i \geq 1$ e sia $s = s(K)$ l'intero tale che $\zeta_s \in K$ e $\zeta_{s+1} \notin K$.

Come nel caso precedente chiamiamo

$$I = \{\ x \in \mathbb{Z} \mid 1 \leq x < pe' \text{ e } (x,p) = 1\}$$

e poniamo $I' = I \cup \{pe'\}$.
Definiamo inoltre $\forall t$ l'applicazione $f(t) = min\{pt,\ t+e\}$.

Sia $I(K) = \{s; \lambda_0, \ldots, \lambda_l\}$ l'invariante associato al campo K come definito nel capitolo 5. Fissiamo $\xi_0, \ldots, \xi_l$ $(l+1)$ elementi di U^1 che soddisfino le ipotesi del lemma di decomposizione 5.3 applicato a ζ_s. Allora:

$$\zeta_s = \xi_0^{p^l}\, \xi_1^{p^{l-1}} \ldots \xi_l$$

con $\lambda_i = v_K(\xi_i - 1) \in I \cup \{pe', +\infty\}$.

Fissiamo una m-pla di interi $\{t^1, \ldots, t^m\}$ che soddisfi le condizioni (a), (b) e (c) del teorema di Miki 5.7, cioè:

(a) t^1 soddisfa una delle due condizioni seguenti:

- $1 \leq t^1 < e'p$ e $t^1 \not\equiv 0(p)$;
- $t^1 = e'p$.

(b) Se $t^i < e'$, t^{i+1} soddisfa una delle 3 condizioni seguenti:

- $t^{i+1} = pt^i$;
- $pt^i < t^{i+1} < e'p$ e $t^{i+1} \not\equiv 0(p)$;
- $t^{i+1} = e'p$.

(c) Se $t^i \geq e'$, allora $t^{i+1} = t^i + e$.

Poniamo inoltre $t^i = 0 \ \forall i \leq 0$.
Come nella sezione precedente distinguiamo il caso $\overline{K} = \mathbb{F}_p$ dal caso $\overline{K} \neq \mathbb{F}_p$.

7.2.1 Caso $\overline{K} = \mathbb{F}_p$

Ricordiamo la definizione della condizione $C(j)$:

$C(j)$ Esiste un sottoinsieme T di $\{0, 1 \dots l\}$ tale che:

- $t^{j-i} = \lambda_{l-i} \quad \forall i \in T$;
- $t^{j-i} < \lambda_{l-i} \quad \forall i \in \{0, 1 \dots l\} - T$,

e la cardinalità dell'insieme T è 1 se $p \neq 2$ e dispari se $p = 2$.

Ricordiamo che il teorema di Miki in questo caso ci dice che esiste un'estensione ciclica totalmente ramificata di grado p^m se e solo se $\{t^1, \dots, t^m\}$ soddisfa le condizioni (a), (b) e (c); inotre, se vale la condizione $C(j)$ per qualche $1 \leq j \leq m$, allora esiste l'estensione ciclica totalmente ramificata di grado p^m con salti della ramificazione $t^1, \dots, t^m$ se e solo se $m \leq j + s - 1$.

Per ognuno dei casi precedenti costruiamo un opportuno sottogruppo N di K^* di indice finito tale che l'estensione associata ad N tramite la corrispondenza della class-field abbia le proprietà richieste.

Fissiamo $t^1 < \dots < t^m$ una m-pla di numeri naturali che soddisfino le condizioni (a),(b) e (c) enunciate prima.
Definiamo i seguenti insiemi:

- $J_1 = \{t_{(1)} < t_{(2)} < \dots < t_{(r)}\} = \{t^i \mid 1 \leq i \leq m\} - \{f(t^i) \mid 1 \leq i \leq m,\ t^i \neq e'\}$;
- $J_2 = \{\lambda_i \mid 0 \leq i \leq l, \lambda_i \neq +\infty\}$;
- $E = \{z \mid 1 \leq z \leq r \text{ e } t_{(z)} \in J_2\}$.

Scriviamo allora $i = i_z$ se $t^i = t_{(z)}$ per qualche $z \in \{1, \dots, r\}$ e $i' = i(z)$ se $t_{(z)} = \lambda_{i'}$ per qualche $z \in E$.

Indichiamo con π un uniformizzante di K. Applicando il teorema 1.9 sappiamo che un U^1 ammette un sistema di generatori $\{\eta_x\}_{x \in I'}$ con $v_K(\eta_x - 1) = x$. A meno di modificare opportunamente gli η_x possiamo supporre che, se $\lambda_i \in I'$ per qualche $0 \leq i \leq l$ allora il generatore di ordine λ_i sia proprio uguale al ξ_i, dove gli ξ_i sono gli elementi che compaiono nella fattorizzazione di ζ_s. Applicando l'osservazione 1.11 al nostro caso si ha che l'unica relazione lineare tra i generatori è

$$(\xi_0^{p^l} \xi_1^{p^{l-1}} \dots \xi_l)^{p^s} = 1.$$

Distinguiamo allora due casi, a seconda che $J_1 \cap J_2 = \varnothing$ oppure $J_1 \cap J_2 \neq \varnothing$.

7.2.2 Caso $J_1 \cap J_2 = \varnothing$

Se $J_1 \cap J_2 = \varnothing$ allora nessuno degli elementi della m-pla dei potenziali salti $\{t^1, \dots, t^m\}$ è uguale ad uno dei λ_i. Facciamo vedere che in questo caso funziona la stessa costruzione fatta nel caso in cui K non contenga radici p-esime dell'unità. Notiamo che, per le condizioni sull'insieme $\{t^1, \dots, t^m\}$, $t^1 \in I' \cap J_1$; di conseguenza $I' \cap J_1 \neq \varnothing$ e, poiché $t^{i_1} = t_{(z)}$, allora $i_1 = 1$.
Chiamiamo inoltre $\eta_{(z)} = \eta_{t(z)}$ $\forall z = 1, \dots, r$ e definiamo $\forall z = 2, \dots, r$, l'elemento ε_z nel modo seguente:

$$\varepsilon_z = \eta_{(1)}^{-p^{iz-1}} \eta_{(z)}.$$

Definiamo allora:

$$N =< K^{*p^m},\ \pi,\ \eta_x \text{ con } x \in I' - J_1,\ \varepsilon_z \text{ se } z = 2, \dots, r > .$$

Vogliamo dimostrare che l'estensione L/K associata al sottogruppo N utilizzando la corrispondenza della class field è ciclica, totalmente ramificata di grado p^m e che ha come salti dell'estensione proprio $\{t^1, \dots, t^m\}$.

- Osserviamo innanzitutto che l'estensione L/K è totalmente ramificata in quanto $\pi \in N$.

- $\zeta_s \in N$ in quanto per ipotesi $J_1 \cap J_2 = \varnothing$ e quindi $\forall i \in \{0, \dots, l\}$ l'elemento $\xi_i \in N$; segue quindi che

$$\zeta_s = \xi_0^{p^l} \xi_1^{p^{l-1}} \dots \xi_l \in N.$$

- Dimostriamo che K^*/N è un gruppo ciclico di ordine p^m e precisamente è generato da $\eta_{(1)}N$.
  Infatti osserviamo innanzitutto che le classi $N, \eta_{(1)}N, \eta_{(1)}^2 N, \dots, \eta_{(1)}^{p^m-1} N$ sono tutte distinte in quanto nessuna delle potenze $\eta_{(1)}^i$ con $i \leq p^m - 1$ appartiene al sottogruppo N. Per mostrare che questi sono gli unici elementi di K^*/N mostriamo che tutti gli altri generatori di U^1 diversi da $\eta_{(1)}$ appartengono ad una delle classi di equivalenza descritte sopra. Distinguiamo dunque due casi:

  - Se η_x è tale che $x \in I' - J_1$, allora $\eta_x \in N$ per costruzione.
  - Se invece η_x è tale che $x \in J_1$ e $x \neq t^1$, allora esiste $z \in \{2, \dots, r\}$ tale che $\eta_x = \eta_{(z)}$. Di conseguenza:

$$\eta_{(z)} = \eta_{(1)}^{p^{iz-1}} \varepsilon_z \in \eta_{(1)}^{p^{iz-1}} N$$

    e banalmente $i_z \leq m$ quindi $\eta_{(1)}^{p^{iz-1}} N$ è una delle classi elencate sopra.

Di conseguenza K^*/N è ciclico di ordine p^m. D'altra parte, dal teorema 3.3 del capitolo 3 si ha che il gruppo di Galois dell'estensione abeliana finita associata ad N è isomorfo a K^*/N, quindi nel nostro caso l'estensione L/K associata ad N è ciclica di grado p^m come voluto.

Per dimostrare che i salti della ramificazione dell'estensione L/K sono esattamente $t^1, \ldots, t^m$ si può utilizzare esattamente lo stesso argomento usato nel caso in cui il campo K non contenga le radici p-esime dell'unità. $\forall 1 \leq i \leq m$ indichiamo con $N_i = NK^{*p^i}$. Per il teorema 6.1 basta quindi dimostrare che $\forall i \in \{1, \ldots, m\}$ si ha $U^{t^i} \not\subset N_i$ e $U^{t^i+1} \subset N_i$.

- Sia u il maggior elemento di $\{1, \ldots, r\}$ tale che $t_{(u)} \leq t_i$.
  Dalla definizione dell'insieme J_1 si ha che $t^i = f(t^{i-1}) = \ldots = f^{i-i_u}(t_{(u)})$.
  Consideriamo $\eta_{(u)}$; abbiamo quindi che:

$$\eta_{(u)} = \begin{cases} \eta_{(1)} \in N_0 - N_1 = N_{i_1-1} - N_{i_1} & \text{se } u = 1 \\ \\ \eta_{(1)}^{p^{i_u-1}} \varepsilon_u \in N_{i_u-1} - N_{i_u} & \text{se } u \geq 2 \end{cases}$$

  Di conseguenza:

  - se $u = 1$ allora $\eta_{(1)}^{p^{i-i_1}} = \eta_{(1)}^{p^{i-1}} \in N_{i-1} - N_i$;
  - se $u \geq 2$

$$\eta_{(u)}^{p^{i-i_u}} = \varepsilon_u^{p^{i-i_u}} (\eta_{(1)}^{p^{i_u-1}})^{p^{i-i_u}} = \varepsilon_u^{p^{i-i_u}} \eta_{(1)}^{p^{i-1}} \in N_{i-1} - N_i.$$

  Abbiamo quindi in ogni caso che $\eta_{(u)}^{p^{i-i_u}} \in N_{i-1} - N_i$.
  D'altra parte

$$v_K(\eta_{(u)}^{p^{i-i_u}} - 1) \geq f^{i-i_u}(v_K(\eta_{(u)} - 1)) = f^{i-i_u}(t_{(u)}) = t^i,$$

  quindi $\eta_{(u)}^{p^{i-i_u}} \in U^{t^i}$ ma $\eta_{(u)}^{p^{i-i_u}} \notin N_i$, come voluto.

- Mostriamo ora che $U^{t^i+1} \subset N_i$.
  $\forall x \geq t^i + 1$ sia n_x il più piccolo intero tale che $x = f^{n_x}(v_x)$ con $v_x \in I'$.
  Distinguiamo due casi:

  - se $v_x \neq t_{(z)} \quad \forall z \in \{1, \ldots, r\}$ allora si ha per costruzione che $\eta_{v_x} \in N$ e quindi anche $\eta_{v_x}^{p^{n_x}} \in N \subset N_i$;

– supponiamo che esista $z \in \{1, \dots, r\}$ tale che $v_x = t_{(z)}$. Abbiamo quindi che:

$$\eta_{v_x} = \eta_{(z)} = \begin{cases} \eta_{(1)} \in N_0 = N_{i_1-1} & \text{se } z = 1 \\ \eta_{(1)}^{p^{i_z-1}} \varepsilon_z \in N_{i_z-1} & \text{se } z \geq 2 \end{cases}$$

Di conseguenza:

* se $z = 1$ allora $\eta_{v_x}^{p^{n_x}} = \eta_{(1)}^{p^{n_x}} \in N_{n_x} = N_{n_x+i_1-1}$;
* se $z \geq 2$ allora

$$\eta_{v_x}^{p^{n_x}} = (\eta_{(1)}^{p^{i_z-1}} \varepsilon_z)^{p^{n_x}} = \eta_{(1)}^{p^{+n_x+i_z-1}} \varepsilon_z^{p^{n_x}} \in N_{n_x+i_z-1};$$

in entrambi i casi vale che $\eta_{v_x}^{p^{n_x}} \in N_{n_x+i_z-1}$. Vogliamo ora dimostrare che $N_{n_x+i_z-1} \subset N_i$. Distinguiamo due casi:

* se $i_z + n_x \geq m + 1$, allora banalmente $i_z + n_x \geq i + 1$, da cui $i_z + n_x - 1 \geq i$;
* se $i_z + n_x \leq m$, allora $t^i + 1 \leq f^{n_x}(t_{(z)}) \leq t^{i_z+n_x}$, da cui si ha quindi che $i + 1 \leq i_z + n_x$ e quindi $i_z + n_x - 1 \geq i$.

Poiché $i_z + n_x - 1 \geq i$ si ha che $N_{n_x+i_z-1} \subset N_i$. D'altra parte osserviamo che U^{t^i+1} è generato come $\mathbb{Z}_p$-modulo dagli elementi della forma $\{\eta_{v_x}^{p^{n_x}}\}_{x \geq t^i+1}$; di conseguenza $U^{t^i+1} \subset N_i$, il che prova che t^i è esattamente l'i-esimo salto della ramificazione in alto dell'estensione associata ad N.

7.2.3 Caso $J_1 \cap J_2 \neq \varnothing$

Se $J_1 \cap J_2 \neq \varnothing$ allora ci sono delle coincidenze tra i $t_{(z)}$ e i λ_i e la situazione è più delicata da trattare. Prima di descrivere la costruzione in questo caso dimostriamo il seguente lemma:

Lemma 7.1. *Valgono le seguenti proprietà:*

1. *Se $t^i = \lambda_{i'}$ per qualche $i \in \{1, \dots, m\}$ e qualche $i' \in \{0, \dots, l\}$, allora $i \in \{i_z \mid z \in E\}$.*

2. *Supponiamo $J_1 \cap J_2 \neq \varnothing$. Siano $z_1 < z_2 < \dots < z_g$ con $g \geq 1$ tali che:*

$$\{z_1, \dots, z_g\} = \{z \in E \mid i_z - i(z) = min\{i_s - i(s) \mid s \in E\}\}.$$

Poniamo $j' = l - i(z_1) + i_{z_1} = \dots = l - i(z_g) + i_{z_g}$. Si ha quindi che $t^{j'-i} \leq \lambda_{l-i}$ $\forall i \in \{0, \dots, l\}$ tale che $j' - i \in \{i_z \mid z \in E\}$ oppure tale che $l - i \in \{i(z) \mid z \in E\}$. Inoltre l'uguaglianza vale esattamente per i g elementi $i = l - i(z_1), \dots, l - i(z_g)$.

3. *Supponiamo che la condizione $C(j)$ valga per qualche $j \in \{1, \dots, m\}$. Allora $J_1 \cap J_2 \neq \emptyset$, $j = j'$ e $g = 1$ se $p \neq 2$ o g è dispari se $p = 2$.*

4. *Supponiamo che $J_1 \cap J_2 \neq \emptyset$ e sia j' definito come al punto 2. Se $g = 1$ nel caso $p \neq 2$ o g dispari nel caso $p = 2$ ma la condizione $C(j')$ non vale allora esiste $h \in \{0, \dots l\}$ tale che $t^{j'-h} > \lambda_{l-h}$, $j' - h \notin \{i_z \mid z \in E\}$ e $l - h \notin \{i(z) \mid z \in E\}$.*

Dimostrazione.

1. Supponiamo che $t^i = \lambda_{i'}$ con $i \in \{1, \dots, m\}$ e $i' \in \{0, \dots, l\}$. Sappiamo che in generale $\lambda_{i'} \in I \cup \{pe', +\infty\}$; d'altra parte per essere uguale ad un t^i si ha $\lambda_{i'} \in I \cup \{pe'\}$. Di conseguenza anche $t^i \in I \cup \{pe'\}$ e quindi è uguale ad uno dei $t_{(z)}$ per costruzione. Si ha dunque che $i \in \{i_z \mid z \in E\}$ (in quanto per costruzione avevamo definito $E = \{\, 1 \leq z \leq r \mid t_{(z)} \in J_2 \,\}$).

2. Sia $s \in \{z_1, \dots, z_g\}$.

   Osserviamo che, se $j' - i = i_z$ per un certo $z \in E$ abbiamo:

   $$t^{j'-i} = t^{i_z} = t_{(z)} = \lambda_{i(z)};$$

   d'altra parte per definizione di $\{z_1, \dots, z_g\}$ si ha che $i_z - i(z) \geq i_s - i(s)$, quindi

   $$t^{j'-i} = \lambda_{i(z)} \leq \lambda_{i_z - i_s + i(s)};$$

   ma per costruzione $j' = l - i(s) + i_s$, dunque sostituendo si ha

   $$t^{j'-i} \leq \lambda_{i_z - i_s + i(s)} = \lambda_{i_z + l - j'} = \lambda_{l-i}$$

   perché $j' - i = i_z$.

   Allo stesso modo, $\forall i \in \{0, \dots, l\}$ tale che $l - i = i(z)$ con $z \in E$ si ha:

   $$\lambda_{l-i} = \lambda_{i(z)} = t_{(z)} = t^{i_z};$$

   ma $i_z - i(z) \geq i_s - i(s)$, quindi

   $$\lambda_{l-i} = t^{i_z} \geq t^{i(z) + i_s - i(s)} = t^{i(z) + j' - l} = t^{j'-i}.$$

Notiamo ora che, se $i = l - i(s)$ con $s \in \{z_1, \dots, z_g\}$, allora vale banalmente l'uguaglianza in quanto

$$t^{j'-i} = t^{i_s} = \lambda_{i(s)} = \lambda_{l-i}$$

Viceversa, se vale l'uguaglianza $t^{j'-i} = \lambda_{l-i}$ allora per definizione esiste $z \in E$ tale che

$$\begin{cases} j' - i = i_z \\ l - i = i(z) \end{cases}$$

Di conseguenza $i = j' + i_z$, quindi sostituendo $l - j' - i_z = i(z)$, cioè $z \in \{z_1, \dots, z_g\}$ e $i = l - i(z)$.

3. Supponiamo che esista $1 \le j \le m$ tale che valga la condizione $C(j)$.
Tale condizione ci dice che l'insieme $T = \{0 \le i \le l \mid t^{j-i} = \lambda_{l-i}\}$ è non vuoto; di conseguenza $J_1 \cap J_2 \neq \varnothing$.
Osserviamo innanzitutto che $j' \le j$. Notiamo infatti che, se $i \in T$ cioé $t^{j-i} = \lambda_{l-i}$, allora esiste $z \in E$ tale che $j - i = i_z$ e $l - i = i(z)$. Combinando insieme queste due relazioni troviamo che $j = l + i_z - i(z)$.
Inoltre, poiché $i_z - i(z) \ge i_{z_1} - i(z_1) = min\{i_t - i(t) \mid t \in E\}$, si ha che $j' = l + i_{z_1} - i(z_1) \le j$.
Supponiamo per assurdo che $j \neq j'$. In generale, se h è un certo indice della forma $h = l - i(s)$ con $s \in \{z_1, \dots, z_g\}$ allora vale l'uguaglianza $t^{j'-h} = \lambda_{l-h} = \lambda_{i(s)}$.
Sia ora $i \in \{0, \dots, l\}$ l'indice tale che $t^{j-i} = t^{j'-h}$; poiché $t^{j'-h} = \lambda_{i(s)}$, si ha che anche $t^{j-i} = \lambda_{i(s)}$, quindi $j - i = i_s$ e dunque $i = j - i_s$. Distinguiamo allora due casi:

- Se $i \in T$, allora $t^{j-i} = \lambda_{l-i}$, quindi $i = h$ e $j' = j$.
- Se $i \notin T$, allora $t^{j-i} < \lambda_{l-i}$. Sostituendo il valore di i otteniamo:

  $$\lambda_{i(s)} = t^{j-i} < \lambda_{l-j+i_s}.$$

  Tuttavia per costruzione abbiamo che i λ_i sono crescenti; di conseguenza

  $$\lambda_{i(s)} < \lambda_{l-j+i_s} \quad \Longleftrightarrow \quad i(s) < l - j + i_s$$

  e ciò vale se e solo se $j' = l + i_s - i(s) > j$, che è assurdo per l'osservazione iniziale.

Abbiamo quindi ottenuto che $j = j'$. Ora, poiché vale la condizione $C(j')$ segue direttamente che la cardinalità dell'insieme T è proprio g, quindi g è uguale ad 1 se $p \neq 2$ oppure è dispari se $p = 2$.

4. Supponiamo che non valga la condizione $C(j')$ anche se vale $g = 1$ se $p \neq 2$ o g dispari se $p = 2$. Allora la condizione che non è verificata è che $t^{j'-i} \leq \lambda_{l-i}$ $\forall i \in \{0, 1, \ldots, l\}$. Di conseguenza esiste $h \in \{0, 1, \ldots, l\}$ tale che $t^{j'-h} > \lambda_{l-h}$. Per quanto dimostrato al punto 2. segue banalmente che $j' - h \notin \{i_z \mid z \in E\}$ e $l - h \notin \{i(z) \mid z \in E\}$, da cui la tesi.

□

Con le proprietà dimostrate nel lemma precedente possiamo descrivere la costruzione anche nel caso in cui $J_1 \cap J_2 \neq \varnothing$.

Siano $z_1 < z_2 < \ldots < z_g$ con $g \geq 1$ tali che:

$$\{z_1, \ldots, z_g\} = \{z \in E \mid i_z - i(z) = min\{i_s - i(s) \mid s \in E\}\ \}.$$

Poniamo $j' = l - i(z_1) + i_{z_1} = \ldots = l - i(z_g) + i_{z_g}$.

Distinguiamo allora tre casi:

(a) $g \geq 2$ nel caso in cui $p \neq 2$ o g pari nel caso in cui $p = 2$;

(b) $g = 1$ nel caso in cui $p \neq 2$ o g dispari nel caso in cui $p = 2$ e vale la condizione $C(j)$ per qualche $j \in \{1, \ldots, m\}$;

(c) $g = 1$ nel caso in cui $p \neq 2$ o g dispari nel caso in cui $p = 2$ e non vale la condizione $C(j')$.

Caso (a)

Supponiamo che $g \geq 2$ nel caso in cui $p \neq 2$ o g pari nel caso in cui $p = 2$.

Dimostriamo il seguente lemma algebrico:

Lemma 7.2. *Nelle ipotesi precedenti esistono $a_z \in \mathbb{Z}$ con $z \in E$ tali che:*

- $a_z \not\equiv 0 \quad (p)$;
- $a_1 = 1$;
- $\sum_{z \in E} a_z p^{i_z - i(z)} = 0$.

Dimostrazione. Distinguiamo due casi:

- Supponiamo $p \neq 2$; allora in questo caso $g \geq 2$.
  Sia $s \in \{z_1, \ldots, z_g\}$ con $s \neq 1$ e definiamo l'insieme $A = \{z_1, \ldots, z_g\} - \{s\}$.
  Possiamo riscivere l'espressione $\sum_{z \in E} a_z p^{i_z - i(z)} = 0$ come:

  $$a_s p^{i_s - i(s)} = -\sum_{z \in A} a_z p^{i_z - i(z)} - \sum_{z \in E - A - \{s\}} a_z p^{i_z - i(z)}.$$

  Definiamo allora $a_z = 1 \ \forall z \in E - A - \{s\}$. Per costruzione sappiamo che $\forall z \in E - A - \{s\}$ vale $i_s - i(s) < i_z - i(z)$; di conseguenza

  $$\sum_{z \in E - A - \{s\}} a_z p^{i_z - i(z)} = p^{i_s - i(s)} k \quad \text{con} \quad k \equiv 0 \ (p).$$

  Dividendo nell'espressione precedente ambo i membri per $p^{i_s - i(s)}$ otteniamo:

  $$a_s = -\sum_{z \in A} a_z - k.$$

  Distinguiamo allora due casi:

  - Se $g - 1 = |A| \not\equiv 0 \ (p)$ possiamo allora porre $a_z = 1 \ \forall z \in A$ e $a_s = -(g-1) - k$, quindi $a_s \equiv -(g-1) \not\equiv 0 \ (p)$, da cui la tesi.
  - Supponiamo $g - 1 = |A| \equiv 0 \ (p)$. Scegliamo $t \in A$ tale che $t \neq 1$ se $1 \in A$; poniamo allora $a_t = 2$ (quindi $a_t \not\equiv 0 \ (p)$ in quanto $p \neq 2$) e $a_z = 1 \ \forall z \in A - \{t\}$. In questo caso allora $a_s = -g - k$, quindi $a_s \equiv -g \not\equiv 0 \ (p)$, da cui la tesi.

- Supponiamo $p = 2$; allora in questo caso g pari.
  Come nel caso precedente sia $s \in \{z_1, \ldots, z_g\}$ con $s \neq 1$ e definiamo l'insieme $A = \{z_1, \ldots, z_g\} - \{s\}$.
  Possiamo riscrivere l'espressione $\sum_{z \in E} a_z 2^{p^{i_z - i(z)}} = 0$ come:

  $$a_s 2^{i_s - i(s)} = -\sum_{z \in A} a_z 2^{i_z - i(z)} - \sum_{z \in E - A - \{s\}} a_z 2^{i_z - i(z)}.$$

  Poniamo allora $a_z = 1 \ \forall z \in E - A - \{s\}$; come nel caso precedente si ha

  $$\sum_{z \in E - A - \{s\}} a_z 2^{i_z - i(z)} = 2^{i_s - i(s)} k \quad \text{con} \quad k \equiv 0 \ (2).$$

  Dividendo nell'espressione precedente ambo i membri per $2^{i_s - i(s)}$ otteniamo:

  $$a_s = -\sum_{z \in A} a_z - k.$$

Poniamo allora $a_z = 1 \forall z \in A$; in questo modo abbiamo quindi che $a_s \equiv -(g-1) \equiv 1\ (2)$ in quanto $g-1$ è dispari, da cui la tesi.

□

Utilzzando il lemma precedente scegliamo alcuni $a_z \in \mathbb{Z}$ con $z \in E$ tali che: $a_z \not\equiv 0\ (p)$, $a_1 = 1$ e $\sum_{z\in E} a_z p^{i_z - i(z)} = 0$. Definiamo inoltre $a_z = 1$ se $z \notin E$.

Poniamo ora $\eta_{(z)} = \eta_{t(z)}\ \forall z \in \{1, \dots, r\}$ e $\varepsilon_z = \eta_{(1)}^{-a_z p^{i_z - i(z)}} \eta_{(z)}\ \forall z \in \{2, \dots, r\}$.

Consideriamo quindi il sottogruppo N di K^* di indice finito definito nel modo seguente:

$$N =< K^{*p^m}, \pi, \eta_x\ (x \in I' - J_1),\ \varepsilon_z\ (z \in \{2, \dots, r\}\ ) > .$$

Vogliamo dimostrare che l'estensione L/K associata al sottogruppo N utilizzando la corrispondenza della class field è ciclica, totalmente ramificata di grado p^m e che ha come salti dell'estensione proprio $\{t^1, \dots, t^m\}$.

- Osserviamo innanzitutto che l'estensione L/K è totalmente ramificata in quanto $\pi \in N$.

- Mostriamo che $\zeta_s \in N$. Sappiamo dalla decomposizione che $\zeta_s = \xi_0^{p^l} \dots \xi_l$ con $v_K(\xi_i - 1) = \lambda_i$ (eventualmente $+\infty$). Allora:

  1. Se $\lambda_i \neq +\infty$ e $\lambda_i \notin J_1 \cap J_2$ allora $\xi_i \in \{\eta_x \mid x \in I' - J_1\}$, quindi $\xi_i \in N$.
  2. Supponiamo ora che $\lambda_i \in J_1 \cap J_2$. In questo caso esiste $z \in E$ tale che $\lambda_{i(z)} = t_{(z)} = t_{i_z}$ e in particolare $\xi_{i(z)}$ è uno degli η_x del tipo $\eta_{(z)}$. Distinguiamo allora due casi:

     - Supponiamo $1 \notin E$. Allora notiamo che

     $$\prod_{z\in E} \varepsilon_z^{p^{l-i(z)}} = \prod_{z\in E} (\eta_{(1)}^{-a_z p^{i_z - 1}})^{p^{l-i(z)}} \eta_{(z)}^{p^{l-i(z)}};$$

     d'altra parte

     $$\prod_{z\in E} \eta_{(z)}^{p^{l-i(z)}} = \prod_{\lambda_h \in J_1 \cap J_2} \xi_h^{p^{l-h}}$$

     e

     $$\prod_{z\in E} (\eta_{(1)}^{-a_z p^{i_z - 1}})^{p^{l-i(z)}} = \prod_{z\in E} (\eta_{(1)}^{-a_z p^{l + i_z - i(z) - 1}})$$
     $$= \left(\prod_{z\in E} \eta_{(1)}^{a_z p^{i_z - i(z)}} \right)^{-p^{l-1}} = \left(\eta_{(1)}^{\sum_{z\in E} a_z p^{i_z - i(z)}} \right)^{-p^{l-1}} = 1.$$

quindi possiamo scrivere ζ_s come:

$$\zeta_s = \prod_{\lambda_i \notin J_1 \cap J_2} \xi_i^{p^{l-i}} \prod_{z \in E} \varepsilon_z^{p^{l-i(z)}}$$

cioè ζ_s è prodotto di elementi di N.

- Supponiamo $1 \in E$. In questo caso $t_{(1)} = t^{i_1} = t^1 = \lambda_{i(1)} = \lambda_1$.

Inoltre:

$$\sum_{z \in E} a_z p^{i_z - i(z)} = \sum_{z \in E - \{1\}} a_z p^{i_z - i(z)} + a_1 p^{i_1 - i(1)} = \sum_{z \in E - \{1\}} a_z p^{i_z - i(z)} + 1,$$

quindi

$$\prod_{z \in E - \{1\}} (\eta_{(1)}^{-a_z p^{i_z - 1}})^{p^{l-i(z)}} = \prod_{z \in E - \{1\}} (\eta_{(1)}^{-a_z p^{l + i_z - i(z) - 1}})$$

$$= \left(\prod_{z \in E - \{1\}} \eta_{(1)}^{a_z p^{i_z - i(z)}} \right)^{-p^{l-1}} = \left(\eta_{(1)}^{\sum_{z \in E - \{1\}} a_z p^{i_z - i(z)}} \right)^{-p^{l-1}} = \eta_{(1)}^{p^{l-1}}.$$

Di conseguenza abbiamo

$$\prod_{z \in E - \{1\}} \varepsilon_z^{p^{l-i(z)}} = \prod_{z \in E - \{1\}} (\eta_{(1)}^{-a_z p^{i_z - 1}})^{p^{l-i(z)}} \eta_{(z)}^{p^{l-i(z)}}$$

$$= \eta_{(1)}^{p^{l-1}} \prod_{z \in E - \{1\}} \eta_{(z)}^{p^{l-i(z)}} = \prod_{\lambda_h \in J_1 \cap J_2} \xi_h^{p^{l-h}} \in N,$$

e quindi possiamo scrivere ζ_s come prodotto di elementi di N:

$$\zeta_s = \prod_{\lambda_i \notin J_1 \cap J_2} \xi_i^{p^{l-i}} \prod_{z \in E} \varepsilon_z^{p^{l-i(z)}}.$$

In entrambi i casi quindi $\zeta_s \in N$.

- Mostriamo che K^*/N è un gruppo ciclico di ordine p^m e precisamente generato da $\eta_{(1)}N$; in questo caso, poichè $\zeta_s \in N$ vale la stessa dimostrazione fatta nel caso in cui $J_1 \cap J_2 = \varnothing$. Segue quindi dalle proprietà della corrispondenza della class field che l'estensione L/K associata ad N è ciclica totalmente ramificata di grado p^m come voluto.

Dimostriamo ora che i salti della ramificazione in alto sono esattamente $t^1, \dots, t^m$.

Come nei casi precedenti definiamo $\forall 1 \le i \le m \ N_i = NK^{*p^i}$. Per il teorema 6.1 basta quindi dimostrare che $\forall i \in \{1, \dots, m\}$ si ha $U^{t^i} \not\subset N_i$ e $U^{t^i+1} \subset N_i$.

- Sia u il maggior elemento di $\{1, \dots, r\}$ tale che $t_{(u)} \le t_i$.
  Dalla definizione dell'insieme J si ha che $t^i = f(t^{i-1}) = \dots = f^{i-i_u}(t_{(u)})$.
  Consideriamo $\eta_{(u)}$; abbiamo quindi che:

$$\eta_{(u)} = \begin{cases} \eta_{(1)} \in N_0 - N_1 = N_{i_1-1} - N_{i_1} & \text{se } u = 1 \\ \\ \eta_{(1)}^{a_z p^{i_u-1}} \varepsilon_u \in N_{i_u-1} - N_{i_u} & \text{se } u \ge 2 \end{cases}$$

  Di conseguenza:

  - se $u = 1$ allora $\eta_{(1)}^{p^{i-i_1}} = \eta_{(1)}^{p^{i-1}} \in N_{i-1} - N_i$;
  - se $u \ge 2$

$$\eta_{(u)}^{p^{i-i_u}} = \varepsilon_u^{p^{i-i_u}} (\eta_{(1)}^{a_z p^{i_u-1}})^{p^{i-i_u}} = \varepsilon_u^{p^{i-i_u}} (\eta_{(1)}^{a_z})^{p^{i-1}} \in N_{i-1} - N_i.$$

  Abbiamo quindi in ogni caso che $\eta_{(u)}^{p^{i-i_u}} \in N_{i-1} - N_i$.
  D'altra parte

$$v_K(\eta_{(u)}^{p^{i-i_u}} - 1) \ge f^{i-i_u}(v_K(\eta_{(u)} - 1)) = f^{i-i_u}(t_{(u)}) = t^i,$$

  quindi $\eta_{(u)}^{p^{i-i_u}} \in U^{t^i}$ e $\eta_{(u)}^{p^{i-i_u}} \notin N_i$, come voluto.

- Dimostriamo ora che $U^{t^i+1} \subset N_i$.
  Indichiamo $\forall x \ge t^i + 1$ con n_x il più piccolo intero tale che $x = f^{n_x}(v_x)$, con $v_x \in I'$. Allora un sistema di generatori di U^{t^i+1} come $\mathbb{Z}_p$ -modulo è dato dagli elementi della forma $\{\eta_{v_x}^{p^{n_x}}\}_{x \ge t^i+1}$. Vogliamo dimostrare quindi che questi elementi appartengono ad N_i.
  Distinguiamo allora due casi:

  - se $v_x \ne t_{(z)} \quad \forall z \in \{1, \dots, r\}$ allora si ha per costruzione che $\eta_{v_x} \in N$ e quindi anche $\eta_{v_x}^{p^{n_x}} \in N \subset N_i$;
  - supponiamo che esista $z \in \{1, \dots, r\}$ tale che $v_x = t_{(z)}$. Abbiamo quindi che:

$$\eta_{v_x} = \eta_{(z)} = \begin{cases} \eta_{(1)} \in N_0 = N_{i_1-1} & \text{se } z = 1 \\ \\ \eta_{(1)}^{a_z p^{i_z-1}} \varepsilon_z = (\eta_{(1)}^{a_z})^{p^{i_z-1}} \varepsilon_z \in N_{i_z-1} & \text{se } z \ge 2 \end{cases}$$

    Di conseguenza:

- se $z = 1$ allora $\eta_{v_x}^{p^{n_x}} = \eta_{(1)}^{p^{n_x}} \in N_{n_x} = N_{n_x+i_1-1}$;
- se $z \geq 2$ allora

$$\eta_{v_x}^{p^{n_x}} = (\eta_{(1)}^{a_z p^{i_z-1}} \varepsilon_z)^{p^{n_x}} = (\eta_{(1)}^{a_z})^{p^{n_x+i_z-1}} \varepsilon_z^{p^{n_x}} \in N_{n_x+i_z-1};$$

in entrambi i casi vale che $\eta_{v_x}^{p^{n_x}} \in N_{n_x+i_z-1}$. D'altra parte, poiché $n_x+i_z-1 \geq i$ (con le stesse considerazioni fatte nei casi precedenti), si ha che $N_{n_x+i_z-1} \subset N_i$, da cui la tesi.

Caso (b)

Supponiamo ora che $g = 1$ se $p \neq 2$ opuure che g sia dispari nel caso in cui $p = 2$ e supponiamo che esista $j \in \{1, \ldots, m\}$ tale che valga la condizione $C(j)$. Dalla condizione 3. del lemma 7.1 abbiamo che $j = j'$. Come nel caso in cui $J_1 \cap J_2 = \varnothing$, definiamo $\eta_{(z)} = \eta_{t(z)}$ $\forall z \in \{1, \ldots, r\}$ e, se $z \in \{2, \ldots, r\}$ poniamo $\varepsilon_z = \eta_{(1)}^{-p^{i_z-1}} \eta_{(z)}$.

Consideriamo allora il sottogruppo N di K^* definito nel modo seguente:

$$N = < K^{*p^m},\ \pi,\ \eta_x \in I' - J_1,\ \varepsilon_z \text{ con } z \in \{2, \ldots, r\} > .$$

Vogliamo dimostrare che l'estensione L/K associata al sottogruppo N utilizzando la corrispondenza della class field è ciclica, totalmente ramificata di grado p^m e che ha come salti dell'estensione proprio $\{t^1, \ldots, t^m\}$.

- Osserviamo innanzitutto che l'estensione L/K è totalmente ramificata in quanto $\pi \in N$.

- Vogliamo dimostrare che K^*/N è ciclico di ordine p^m e che precisamente è generato da $\eta_{(1)}N$. Indichiamo ora con D l'insieme $\{0, 1, \ldots, l\} - \{i(z) \mid z \in E\}$ e definiamo

$$B = \sum_{z \in E} p^{l-i(z)+i_z-1}.$$

Notiamo che in questo caso ζ_s può essere scritto come

$$\zeta_s = \eta_{(1)}^B \prod_{z \in E-\{1\}} \varepsilon_z^{p^{l-i(z)}} \prod_{i \in D} \xi_i^{p^{l-i}};$$

infatti:

– Se $1 \notin E$ allora

$$\eta_{(1)}^{B} \prod_{z\in E} \varepsilon_z^{p^{l-i(z)}} = \eta_{(1)}^{B} \prod_{z\in E} \eta_{(1)}^{p^{l-i(z)+i_z-1}} \eta_{(z)}^{p^{l-i(z)}} = \prod_{\{i(z) \mid z\in E\}} \xi_{i(z)}^{p^{l-i(z)}},$$

da cui

$$\zeta_s = \prod_{z\in E} \xi_{i(z)}^{p^{l-i(z)}} \prod_{i\in D} \xi_i^{p^{l-i}} = \eta_{(1)}^{B} \prod_{z\in E} \varepsilon_z^{p^{l-i(z)}} \prod_{i\in D} \xi_i^{p^{l-i}}$$

– Se $1 \in E$ allora

$$\eta_{(1)}^{B} \prod_{z\in E-\{1\}} \varepsilon_z^{p^{l-i(z)}} = \eta_{(1)}^{B} \prod_{z\in E-\{1\}} \eta_{(1)}^{p^{l-i(z)+i_z-1}} \eta_{(z)}^{p^{l-i(z)}} = \eta_{(1)}^{p^{l-1}} \prod_{z\in E-\{1\}} \eta_{(z)}^{p^{l-i(z)}}.$$

da cui

$$\eta_{(1)}^{B} \prod_{z\in E-\{1\}} \varepsilon_z^{p^{l-i(z)}} = \prod_{z\in E} \eta_{(z)}^{p^{l-i(z)}} = \prod_{\{i(z) \mid z\in E\}} \xi_{i(z)}^{p^{l-i(z)}}$$

e quindi

$$\zeta_s = \prod_{z\in E} \xi_{i(z)}^{p^{l-i(z)}} \prod_{i\in D} \xi_i^{p^{l-i}} = \eta_{(1)}^{B} \prod_{z\in E-\{1\}} \varepsilon_z^{p^{l-i(z)}} \prod_{i\in D} \xi_i^{p^{l-i}}.$$

In questo caso abbiamo quindi che $\zeta_s \equiv \eta_{(1)}^{B}\ (N)$. Osserviamo ora che il massimo esponente α tale che p^α divide B è esattamente $j' - 1$.
Infatti se chiamiamo $F = \{z_1, \ldots, z_g\}$ allora possiamo riscrivere B come:

$$B = \sum_{z\in E} p^{l-i(z)+i_z-1} = \sum_{z\in F} p^{j'-1} + \sum_{z\in E-F} p^{l-i(z)+i_z-1} = gp^{j'-1} + \sum_{z\in E-F} p^{l-i(z)+i_z-1}$$

perché da costruzione $j' = l - i(z_1) + i_{z_1} = \ldots = l - i(z_g) + i_{z_g}$.
Inoltre $\forall z \in E - F$ si ha che $j' - 1 < l - i(z) + i_z - 1$, quindi

$$\sum_{z\in E-F} p^{l-i(z)+i_z-1} = p^{j'-1}k \quad \text{con} \quad k \equiv 0\ (p).$$

D'altra parte per le proprietà di g si ha che $g \not\equiv 0\ (p)$, quindi $p^{j'-1} \parallel B$ cioè $B = p^{j'-1}b$ con $(b, p) = 1$. La relazione lineare in questo caso diventa

$$1 = (\eta_{(1)}^{b})^{p^{j'+s-1}} \Big(\prod_{z\in E-\{1\}} \varepsilon_z^{p^{l-i(z)}} \prod_{i\in D} \xi_i^{p^{l-i}} \Big)^{p^s}.$$

Poiché dalla condizione di Miki $j' + s - 1 \geq m$, si ha che $\eta_{(1)} \notin N$ e l'ordine di $eta_{(1)}N$ in K^*/N è $\eta_{(1)}N$ è K^{*p^m}. Per dimostrare che il gruppo K^*/N è esattamente di grado p^m dimostriamo che gli altri generatori η_x appartengono ad una delle classi precedenti. Come prima distinguiamo due casi:

- Supponiamo che $x \in I' - J_1$; allora $\eta_x \in N$ per costruzione.
- Se invece η_x è tale che $x \in J_1$ e $x \neq t^1$, allora esiste $z \in \{2, \dots, r\}$ tale che $\eta_x = \eta_{(z)}$. Di conseguenza:

$$\eta_{(z)} = \eta_{(1)}^{p^{i_z-1}} \varepsilon_z \in \eta_{(1)}^{p^{i_z-1}} N$$

e banalmente $i_z \leq m$ quindi $\eta_{(1)}^{p^{i_z-1}} N$ è una delle classi elencate sopra.

Di conseguenza K^*/N è ciclico di ordine p^m con generatore $\eta_{(1)}N$. D'altra parte per le proprietà della corrispondenza data dalla class field si ha che l'estensione L/K associata ad N è ciclica di grado p^m come voluto.

Dimostriamo ora che i salti della ramificazione dell'estensione L/K sono esattamente $t^1, \dots, t^m$.

$\forall 1 \leq i \leq m$ indichiamo con $N_i = NK^{*p^i}$. Come nei casi precedenti basta quindi dimostrare che $\forall i \in \{1, \dots, m\}$ si ha $U^{t^i} \notin N_i$ e $U^{t^i+1} \subset N_i$. Osserviamo ora che il gruppo N appena considerato ha la stessa forma del gruppo usato nella costruzione fatta nel caso in cui $J_1 \cap J_2 = \varnothing$, e che la dimostrazione del fatto che $U^{t^i} \notin N_i$ e $U^{t^i+1} \subset N_i$ dipende soltanto dalla forma del gruppo e non dalla classe di ζ_s modulo N. Di conseguenza applicando esattamente la stessa dimostrazione fatta nel caso $J_1 \cap J_2 = \varnothing$ si ha che N soddisfa le proprietà richieste.

Caso (c)

Supponiamo ora che $g = 1$ nel caso in cui $p \neq 2$ oppure g dispari nel caso in cui $p = 2$ e che la condizione $C(j')$ non sia verificata.
Dal punto 4. del lemma 7.1 abbiamo visto che esiste $h \in \{0, \dots, l\}$ tale che $t^{j'-h} > \lambda_{l-h}$, $j' - h \notin \{i_z \mid z \in E\}$ e $l - h \notin \{i(z) \mid z \in E\}$.
Poniamo $\eta_{(z)} = \eta_{t(z)}$ se $z = \{1, \dots r\}$ e $\varepsilon_z = \eta_{(1)}^{-p^{i_z-1}} \eta_{(z)}$ se $z \in \{2, \dots, r\}$. Definiamo inoltre:

$$A = \sum_{z \in E} p^{l-i(z)+i_z-1-h} \quad \text{e} \quad \eta_0 = \eta_{\lambda_{l-h}} \eta_{(1)}^A.$$

Osserviamo che A è intero. Infatti l'elemento h del lemma 7.1 è tale che $t^{j'-h} > \lambda_{l-h}$, quindi $t^{j'-h} > 0$ e cioè $1 \leq j' - h \leq m$. Si ha quindi che, se $s \in \{z_1, \dots, z_g\}$, allora $\forall z \in E$

$$l - i(z) + i_z - 1 - h \geq l + i_s - i(s) - 1 - h = j' - 1 - h \geq 0,$$

quindi

$$A = \sum_{z \in E} p^{l-i(z)+i_z-1-h} \in \mathbb{Z},$$

da cui η_0 è un elemento di K.

Consideriamo allora il sottogruppo N di K^* definito nel modo seguente:

$$N =< K^{*p^m}, \pi, \eta_x \ (x \in I' - J_1 - \lambda_{l-h}), \ \eta_0, \varepsilon_z \ (z = 2, \ldots, r) >$$

Vogliamo dimostrare che l'estensione L/K associata al sottogruppo N utilizzando la corrispondenza della class field è ciclica, totalmente ramificata di grado p^m e che ha come salti dell'estensione proprio $\{t^1, \ldots, t^m\}$.

- Osserviamo innanzitutto che l'estensione L/K è totalmente ramificata in quanto $\pi \in N$.

- Dimostriamo che $\zeta_s \in N$. Sia V l'insieme di indici definito nel modo seguente:
$$V = \{0, 1, \ldots, l\} - \{i(z) \mid z \in E\} - \{\lambda_{l-h}\};$$
possiamo allora riscrivere la fattorizzazione di ζ_s nel modo seguente:
$$\zeta_s = \xi_{l-h}^{p^h} \prod_{i \in V} \xi_i^{p^{l-i}} \prod_{j \in \{i(z) \mid z \in E\}} \xi_j^{l-j}.$$
Notiamo allora che, se $i \in V$ allora esiste $x \in I' - J_1 - \{\lambda_{l-h}\}$ tale che $\xi_i = \eta_x$; dalla costruzione di N si ha quindi $\eta_x \in N$. Di conseguenza
$$\prod_{i \in V} \xi_i^{p^{l-i}} \in N.$$
Osserviamo inoltre che
$$\begin{aligned} \eta_0^{p^h} \prod_{z \in E} \varepsilon_z^{p^{l-i(z)}} &= (\eta_{(1)}^A)^{p^h} \eta_{\lambda_{l-h}}^{p^h} \prod_{z \in E} (\eta_{(1)}^{-p^{i_z-1}})^{p^{l-i(z)}} \eta_{(z)}^{p^{l-i(z)}} \\ &= \eta_{(1)}^{\sum_{z \in E} p^{l-i(z)+i_z-1}} \eta_{\lambda_{l-h}}^{p^h} \eta_{(1)}^{-\sum_{z \in E} p^{l-i(z)+i_z-1}} \prod_{z \in E} \eta_{(z)}^{p^{l-i(z)}} \\ &= \eta_{\lambda_{l-h}}^{p^h} \prod_{z \in E} \eta_{(z)}^{p^{l-i(z)}} = \xi_{l-h}^{p^h} \prod_{j \in \{i(z) \mid z \in E\}} \xi_j^{l-j}. \end{aligned}$$
Di conseguenza
$$\xi_{l-h}^{p^h} \prod_{j \in \{i(z) \mid z \in E\}} \xi_j^{l-j} \in N$$
perché prodotto di elementi di N, da cui $\zeta_s \in N$.

- Dimostriamo che K^*/N è un gruppo ciclico di ordine p^m e precisamente generato da $\eta_{(1)}N$.
  Infatti abbiamo dimostrato che $\zeta_s \in N$; inoltre le classi N, $\eta_{(1)}N$, $\eta_{(1)}^2N$, $\ldots$, $\eta_{(1)}^{p^m-1}N$ sono tutte distinte in quanto nessuna delle potenze $\eta_{(1)}^i$ con $i \leq p^m - 1$ appartiene al sottogruppo N.
  Per mostrare che questi sono gli unici elementi di K^*/N mostriamo che tutti gli altri generatori di U^1 diversi da $\eta_{(1)}$ appartengono ad una delle classi di equivalenza descritte sopra. Distinguiamo dunque tre casi:

  - Se η_x è tale che $x \in I' - J_1 - \{\lambda_{l-h}\}$, allora $\eta_x \in N$ per costruzione.
  - Se η_x è tale che $x \in J_1$ e $x \neq t^1$, allora esiste $z \in \{2, \ldots, r\}$ tale che $\eta_x = \eta_{(z)}$. Di conseguenza:

    $$\eta_{(z)} = \eta_{(1)}^{p^{iz-1}} \varepsilon_z \in \eta_{(1)}^{p^{iz-1}} N.$$

  - Se infine $x = \lambda_{l-h}$ allora

    $$\eta_{\lambda_{l-h}} = \eta_{(1)}^{-A}\eta_0 = \eta_{(1)}^{-A}N.$$

  Di conseguenza K^*/N è ciclico di ordine p^m e per le proprietà date dalla class field l'estensione L/K associata ad N è ciclica di grado p^m come voluto.

Dimostriamo ora che i salti della ramificazione dell'estensione L/K sono esattamente $t^1, \ldots, t^m$.

$\forall 1 \leq i \leq m$ indichiamo con $N_i = NK^{*p^i}$. Come nei casi precedenti basta dimostrare che $\forall i \in \{1, \ldots, m\}$ si ha $U^{t^i} \not\subset N_i$ e $U^{t^i+1} \subset N_i$. Notiamo che anche in questo caso per dimostrare che $U^{t^i} \not\subset N$ si può usare lo stesso ragionamento del caso $J_1 \cap J_2 = \varnothing$ (se u è il maggior elemento di $\{1, \ldots, r\}$ tale che $t_{(u)} \leq t_i$ allora si dimostra che $\eta_{(u)}^{p^{i-i_u}}$ è un elemento di u^{t^i} che non appartiene a N_i).
Mostriamo ora che $U^{t^i+1} \subset N_i$.
$\forall x \geq t^i + 1$ sia n_x il più piccolo intero tale che $x = f^{n_x}(v_x)$ con $v_x \in I'$. Come osservato anche nei casi precedenti, un insieme di generatori di U^{t^i+1} come $\mathbb{Z}_p$-modulo è dato dagli elementi della forma $\{\eta_{v_x}^{p^{n_x}}\}_{x \geq t^i+1}$. Basta quindi dimostrare che $\forall x \geq t^i + 1$ si ha $\eta_{v_x}^{p^{n_x}} \in N_i$. Distinguiamo dunque tre casi:

- se $v_x \neq t_{(z)} \quad \forall z \in \{1, \ldots, r\}$ e $v_x \neq \lambda_{l-h}$ allora si ha per costruzione che $\eta_{v_x} \in N$ e quindi anche $\eta_{v_x}^{p^{n_x}} \in N \subset N_i$.

- Supponiamo $v_x = \lambda_{l-h}$. Dal punto 4. del lemma 7.1 abbiamo banalmente che $v_x \neq t_{(z)} \ \forall z \in \{1, \ldots, r\}$. Inoltre osserviamo che l'esatto esponente

α tale che $p^{\alpha} \mid A$ è esattamente $j' - 1 - h$.
Infatti chiamiamo $T = \{z_1, \ldots, z_g\}$; possiamo riscrivere A nel modo seguente:

$$\begin{aligned} A &= \sum_{z \in E} p^{l-i(z)+i_z-1-h} = \sum_{z \in T} p^{j'-1-h} + \sum_{z \in E-T} p^{l-i(z)+i_z-1-h} \\ &= g p^{j'-1-h} + \sum_{z \in E-T} p^{l-i(z)+i_z-1-h}. \end{aligned}$$

D'altra parte se $z \in E - T$ allora $l - i(z) + i_z - 1 - h > j' - 1 - h$, quindi

$$\sum_{z \in E-T} p^{l-i(z)+i_z-1-h} \equiv 0 \mod (p^{j'-h})$$

e dalle ipotesi su g sappiamo che $g \not\equiv 0\ (p)$, dunque $g p^{j'-1-h} \not\equiv 0\ (p^{j'-h})$.
Segue allora che $p^{j'-1-h} \parallel A$.
Applicando ciò si ha che $\eta_{v_x} \in \eta_{(1)}^{-A} N \subset N_{j'-1-h}$, da cui $\eta_{v_x}^{p^{n_x}} \in N_{j'-h+n(x)-1}$.
Osserviamo ora che:

- se $j' - h + n(x) - 1 \geq m + 1$ allora banalmente $j' - h + n(x) - 1 \geq i$ e quindi $\eta_{v_x}^{p^{n_x}} \in N_{j'-h+n(x)-1} \subset N_i$;
- se invece $j' - h + n(x) - 1 \leq m$ allora

$$t^i + 1 \leq x = f^{p^{n_x}}(v_x) = f^{n_x}(\lambda_{l-h}) < f^{n_x}(t^{j'-h}) \leq t^{j'-h+n(x)}$$

e quindi $j' - h + n(x) \geq i + 1$, da cui $N_{j'-h+n(x)-1} \subset N_i$.

- Supponiamo infine che esista $z \in \{1, \ldots, r\}$ tale che $v_x = t_{(z)}$. Abbiamo quindi che:

$$\eta_{v_x} = \eta_{(z)} = \begin{cases} \eta_{(1)} \in N_0 = N_{i_1-1} & \text{se } z = 1 \\ \eta_{(1)}^{p^{i_z-1}} \varepsilon_z \in N_{i_z-1} & \text{se } z \geq 2 \end{cases}$$

Di conseguenza in entrambi i casi vale che $\eta_{v_x}^{p^{n_x}} \in N_{n_x+i_z-1}$. Vogliamo ora dimostrare che $N_{n_x+i_z-1} \subset N_i$. Ma già nei casi precedenti avevamo visto che $i_z + n_x - 1 \geq i$; vale quindi che $N_{n_x+i_z-1} \subset N_i$, da cui $\eta_{v_x}^{p^{n_x}} \in N_i$.

Anche in questo caso abbiamo quindi che i salti dell'estensione L/K sono esattamente $\{t^1, \ldots, t^m\}$, da cui si ha la tesi.

7.2.4 Caso $\overline{K} \neq \mathbb{F}_p$

Vogliamo generalizzare i ragionamenti della sezione precedente per costruire i sottogruppi normici nel caso in cui $\overline{K} \neq \mathbb{F}_p$ in modo analogo a quanto

fatto nel caso in cui $\zeta_p \notin K$. Supponiamo che il grado di inerzia di K sia $f > 1$. In questo caso allora il campo dei residui sarà $\overline{K} = \mathbb{F}_q$ con $q = p^f$ e sappiamo che $\overline{K}$ è uno spazio vettoriale su $\mathbb{F}_p$ di dimensione f.
Ricordiamo che in questo caso il teorema di Miki dice che data $\{t^1, \dots, t^m\}$ una m-pla di interi allora esiste un'estensione ciclica totamente ramificata di grado p^m se e solo se l'insieme $\{t^1, \dots, t^m\}$ soddisfa le condizioni (a), (b) e (c) del teorema di Miki; inoltre se vale la condizione

$$D(I): \quad t^I = \lambda_l = pe', \ t^{I-1} < e' \text{ e } t^{I-i} < \lambda_{l-i} \ \forall i = 1, \dots, l$$

per qualche $\leq I \leq m$, allora esiste l'estensione esiste se e solo se $m \leq I + s - 1$.

Fissiamo allora una m-pla di interi $\{t^1, \dots, t^m\}$ che soddisfi le condizioni $(a), (b)$ e (c) del teorema di Miki.
Indichiamo con J il seguente insieme:

$$J = \{t_{(1)}, \dots, t_{(r)}\} = \{t^1, \dots, t^m\} - \{f(t^i) \mid i = 1, \dots, m\}$$

e con $I = \{1 \leq x < pe/(p-1) \mid (x, p) = 1\}$ e $I' = I \cup \{pe'\}$.
Scriviamo allora $i = i_z$ se $t^i = t_{(z)}$ per qualche $z \in \{1, \dots, r\}$ e $i' = i(z)$ se $t_{(z)} = \lambda_{i'}$ per qualche $z \in \{1, \dots, r\}$.

Osservazione 7.3. Dalla definizione dell'insieme J si vede che, se la condizione $D(I)$ vale per un qualche $1 \leq I \leq m$ allora necessariamente $I = i_r$. Infatti, poiché deve valere $t_I = pe'$ e $t_{I-1} < e'$, allora pe' banalmente è un elemento dell'insieme J. Inoltre è il massimo dell'insieme J in quanto per le condizioni del teorema di Miki si vede che se $t^h > pe'$ per qualche h allora $t^{h-1} = t^h - e$. Di conseguenza t^h appartiene all'insieme $\{f(t^i) \mid i = 1, \dots, m\}$ e quindi $t^h \notin J$.

Definiamo inoltre l'insieme

$$F = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x \in I, \ 1 < y < f\} \quad \text{e} \quad F' = F \cup \{(pe', 1)\}.$$

Siano $a_1 \dots a_f$ f elementi di K tali che le rispettive riduzioni $\overline{a}_1, \dots \overline{a}_f$ siano una base di $\overline{K}$ come spazio vettoriale su $\mathbb{F}_p$. Utilizzando il teorema 1.9 si ha che, se indichiamo con $\eta_{(x,y)} = 1 + a_y \pi^x$, dove π è un uniformizzante di $\overline{K}$ e $(x, y) \in F$ e con $\eta_{(pe',1)} = 1 + \pi^{pe'}$, l'insieme $\{\eta_{(x,y)}\}_{(x,y) \in F'}$ costituisce un sistema di generatori di U^1 come $\mathbb{Z}_p$-modulo (nel caso in cui il campo dei residui sia finito e K contenga le radici p-esime dell'unità sappiamo infatti che $\psi(\overline{K})$ è di indice p in $\overline{K}$). A meno di modificare opportunamente i generatori possiamo prendere gli $\eta_{(x,y)}$ tali che

$$\eta_{(x,f)} = \xi_i \text{ se } x = \lambda_i \in I \quad \text{e} \quad \eta_{(pe',1)} = \xi_l \text{ se } \lambda_l = pe'.$$

Inoltre, per l'osservazione 1.11 sappiamo che l'unica relazione di dipendenza lineare è

$$(\xi_0^{p^l}\xi_1^{p^{l-1}}\dots\xi_l)^{p^s} = 1.$$

Indichiamo con F_1 l'insieme $\{(t_{(z)}, 1) \mid 1 \le z \le r\}$.

Distinguiamo allora due casi principali, a seconda che $t_{(r)} = \lambda_l = pe'$ oppure no.

7.2.5 Caso $t_{(r)} \neq pe'$ oppure $\lambda_l \neq pe'$

Supponiamo che $t_{(r)} \neq pe'$ oppure $\lambda_l \neq pe'$. In questo caso la costruzione risulta identica a quella fatta nel caso in cui $\zeta_p \notin K$. Infatti $\forall z \in \{1, \dots, r\}$, poniamo

$$\eta_{(z)} = \eta_{(t_{(z)},1)} \quad \text{e} \quad \varepsilon_z = \eta_{(1)}^{-p^{iz-1}}\eta_{(z)}.$$

Consideriamo allora il sottogruppo N di K^* definito nel modo seguente:

$$N =< K^{*p^m}, \pi, \eta_{(x,y)} \text{ con } x \in F - F_1, \varepsilon_z \text{ se } z = 2, \dots, r > .$$

Dimostriamo che l'estensione L/K associata al sottogruppo N utilizzando la corrispondenza della class field è ciclica, totalmente ramificata di grado p^m e che ha come salti dell'estensione proprio $\{t^1, \dots, t^m\}$. Infatti:

- Poiché $\pi \in N$ l'estensione associata ad N è totalmente ramificata.
- Mostriamo che $\zeta_s \in N$.
  Osserviamo banalmente che se $i \in \{0, \dots, l-1\}$ allora $\xi_i = \eta_{(\lambda_i,f)} \in N$ in quanto $(\lambda_i, f) \in F - F_1$. Inoltre:
  - se $\lambda_l \neq pe'$ allora $\xi_l = \eta_{(\lambda_l,f)} \in N$ in quanto $(\lambda_l, f) \in F - F_1$;
  - se invece $\lambda_l = pe'$ allora si ha che $t_{(r)} \neq pe'$ e quindi $\xi_l = \eta_{(pe',1)} \in N$ in quanto $(pe', 1) \in F - F_1$.

  Di conseguenza $\zeta_s = \xi_0^{p^l}\xi_1^{p^{l-1}}\dots\xi_l \in N$ perché prodotto di elementi di N.
- Il gruppo K^*/N è ciclico di ordine p^m ed è generato dall'elemento $\eta_{(1)}N$.
  Infatti osserviamo che anche in questo caso le classi N, $\eta_{(1)}N$, $\eta_{(1)}^2N$, $\dots$, $\eta_{(1)}^{p^m-1}N$ sono tutte distinte in quanto nessuna delle potenze $\eta_{(1)}^i$ con $i \le p^m - 1$ appartiene al sottogruppo N.
  Per mostrare che non ci sono altre classi mostriamo che ognuno dei generatori di U^1 diverso da $\eta_{(1)}$ è in una delle classi elencate sopra. Consideriamo allora $\eta_{(x,y)}$ e distinguiamo due casi:
  - se $(x, y) \in F - F_1$ allora $\eta_{(x,y)} \in N$ per costruzione;

– supponiamo $(x, y) \in F_1$; allora $y = 1$ ed esiste $z \in \{2, \dots r\}$ tale che $\eta_{(x,y)} = \eta_{(z)}$. In questo caso allora

$$\eta_{(x,y)} = \eta_{(z)} = \eta_{(1)}^{p^{i_z-1}} \varepsilon_z \in \eta_{(1)}^{p^{i_z-1}} N$$

ed essendo banalmente $i_z \leq m$ si ha che $\eta_{(1)}^{p^{i_z-1}} N$ è una delle classi descritte sopra.

Di conseguenza K^*/N è un gruppo ciclico di grado p^m e l'estensione associata è ciclica di grado p^m per le proprietà della teoria della class field.

Per mostrare che i salti sono esattamente $\{t^1, \dots, t^m\}$ si usa come al solito il teorema 6.1; chiamiamo $N_i = NK^{*p^i}$ $\forall 1 \leq i \leq m$. Basta quindi dimostrare che $\forall i \in \{1, \dots, m\}$ si ha $U^{t^i} \not\subset N_i$ e $U^{t^i+1} \subset N_i$. In questo caso la dimostrazione delle due proprietà è identica a quella fatta nel caso in cui $\overline{K} \neq \mathbb{F}_p$ e $\zeta_p \notin K$ (a meno di sostituire l'insieme I' all'insieme I).

7.2.6 Caso $t_{(r)} = \lambda_l = pe'$

Sotto questa ipotesi la costruzione risulta più complicata e dobbiamo distinguere tre ulteriori sottocasi.

Caso a

Supponiamo che $t^{i_r} = \lambda_l = pe'$ e che $t^{i_r-i} \leq \lambda_{l-i}$ $\forall i = 1, 2, \dots, l$. Supponiamo inoltre che esista H tale che $H \in \{1, \dots, l\}$ che soddisfi $t^{i_r-H} = \lambda_{l-H}$; sia allora $1 \leq w \leq r-1$ tale che $t_{(w)} = t^{i_r-H} = \lambda_{l-H} = \lambda_{i(w)}$.
Poniamo quindi:

- $\eta_{(z)} = \eta_{(t_{(z)},1)}$ se $1 \leq z \leq r$ e $z \neq w$;
- $\eta_{(w)} = \eta_{(t_{(w)},f)}$;
- $\varepsilon_z = \eta_{(1)}^{-p^{i_z-1}} \eta_{(z)}$ se $2 \leq z \leq r-1$;
- $\varepsilon_r = \eta_{(1)}^{p^{i_r-1}} \eta_{(r)}$;
- $F_1' = \{(t_{(z)}, 1) \mid 1 \leq z \leq r,\ z \neq w\} \cup \{(t_{(w)}, f)\}$.

Consideriamo allora il sottogruppo N di K^* definito nel modo seguente:

$$N =< K^{*p^m}, \pi, \eta_{(x,y)} \text{ con } x \in F - F_1', \varepsilon_z \text{ se } z = 2, \dots, r > .$$

Dimostriamo che l'estensione L/K associata al sottogruppo N utilizzando la corrispondenza della class field è ciclica, totalmente ramificata di grado p^m e che ha come salti dell'estensione proprio $\{t^1, \dots, t^m\}$. Infatti:

- Poiché $\pi \in N$ l'estensione associata ad N è totalmente ramificata.
- Mostriamo che $\zeta_s \in N$.
  Sappiamo infatti dal lemma di decomposizione che

  $$\zeta_s = \xi_l \dots \xi_0^{p^l}.$$

  Per come abbiamo scelto il sistema di generatori di U_K^1 sappiamo che $\eta_{(x,f)} = \xi_i$ se $x = \lambda_i \in I$ e $\eta_{(pe',1)} = \xi_l$ se $\lambda_l = pe'$. Di conseguenza se $i \neq l$ e $i \neq i(w)$ si ha che per costruzione $\xi_i \in N$. Possiamo scrivere quindi ζ_s come:

  $$\zeta_s = \xi_l \xi_{i(w)}^{p^{l-i(w)}} \prod_{0 \leq i \leq l-1,\ i \neq i(w)} \xi^{p^{l-i}}.$$

  Basta allora dimostrare che $\xi_l \xi_{i(w)}^{p^{l-i(w)}} \in N$. Notiamo che per la condizione su H si ha che $i_w = i_r - H$ e $i(w) = l - H$, da cui $l - i(w) = H = i_r - i_w$. Calcoliamo quindi $\varepsilon_r \varepsilon_w^{p^{i_r - i_w}}$:

  $$\begin{aligned} \varepsilon_r \varepsilon_w^{p^{i_r - i_w}} &= \eta_{(1)}^{p^{i_r - 1}} \eta_{(r)} \left(\eta_{(1)}^{-p^{i_w - 1}} \eta_{(w)}\right)^{p^{i_r - i_w}} \\ &= \eta_{(1)}^{p^{i_r - 1}} \xi_l \ \eta_{(1)}^{-p^{i_r - 1}} \xi_{i(w)}^{p^H} = \xi_l \ \xi_{i(w)}^{p^{l - i(w)}}. \end{aligned}$$

  Di conseguenza $\zeta_s \in N$ perché prodotto di elementi di N.
- Il gruppo K^*/N è ciclico di ordine p^m ed è generato dall'elemento $\eta_{(1)}N$. Infatti osserviamo che anche in questo caso le classi N, $\eta_{(1)}N$, $\eta_{(1)}^2 N$, $\dots$, $\eta_{(1)}^{p^m - 1} N$ sono tutte distinte in quanto nessuna delle potenze $\eta_{(1)}^i$ con $i \leq p^m - 1$ appartiene al sottogruppo N. Inoltre poiché $\eta_{(1)}^{p^m} \in N$ queste sono le uniche classi distinte di potenze di $\eta_{(1)}$.
  Per mostrare che non ci sono altre classi mostriamo che ognuno dei generatori di U^1 diverso da $\eta_{(1)}$ è in una delle classi elencate sopra. Consideriamo allora $\eta_{(x,y)}$ e distinguiamo due casi:
  - se $(x, y) \in F - F_1'$ allora $\eta_{(x,y)} \in N$ per costruzione;
  - supponiamo $(x, y) \in F_1'$; esiste $z \in \{2, \dots r\}$ tale che $\eta_{(x,y)} = \eta_{(z)}$. Distinguiamo due casi:
    * Se $z \neq r$ allora:

      $$\eta_{(t_{(z)},y)} = \eta_{(z)} = \eta_{(1)}^{p^{i_z - 1}} \varepsilon_z \in \eta_{(1)}^{p^{i_z - 1}} N.$$

∗ Se $z = r$ allora $y = 1$. In questo caso dunque:

$$\eta_{(t_{(r)},1)} = \eta_{(r)} = \eta_{(1)}^{-p^{i_r-1}} \varepsilon_r \in \eta_{(1)}^{-p^{i_z-1}} N.$$

Di conseguenza K^*/N è un gruppo ciclico di grado p^m e l'estensione associata è ciclica di grado p^m per le proprietà della teoria della class field.

Per mostrare che i salti sono esattamente $\{t^1, \dots, t^m\}$ si usa come al solito il teorema 6.1; chiamiamo $N_i = NK^{*p^i}$ $\forall 1 \le i \le m$. Basta quindi dimostrare che $\forall i \in \{1, \dots, m\}$ si ha $U^{t^i} \not\subset N_i$ e $U^{t^i+1} \subset N_i$. La dimostrazione della proprietà $U^{t^i} \not\subset N_i$ è identica a quella nel caso in cui $\overline{K} \neq \mathbb{F}_p$ e $\zeta_p \notin K$ (anche qui basta prendere u il maggior elemento di $\{1, \dots, r\}$ tale che $t_{(u)} \le t_i$ e si dimostra allo stesso modo che $\eta_{(u)}^{p^{i-i_u}}$ è un elemento di U^{t^i} che non appartiene ad N_i).
Dimostriamo allora che $U^{t^i+1} \subset N_i$.
$\forall x \ge t^i + 1$ sia n_x il più piccolo intero tale che $x = f^{n_x}(v_x)$ con $v_x \in I'$. Notiamo allora che in questo caso U^{t^i+1} è generato dagli elementi della forma $\{\eta_{(v_x,y)}^{p^{n_x}}\}$ con $x \ge t^i + 1$ e y varia nell'insieme $\{1, \dots, f\}$ se $v_x \neq pe'$ oppure è uguale ad 1 se $v_x = pe'$. Vogliamo mostrare che gli elementi di questa forma appartengono a N_i. Distinguiamo allora due casi:

- supponiamo che $v_x \neq t_{(z)} \quad \forall z \in \{1, \dots, r\}$; allora si ha per costruzione che $\eta_{(v_x,y)} \in N \ \forall y \in \{1, \dots, f\}$ e quindi anche $\eta_{v_x}^{p^{n_x}} \in N \subset N_i$;
- supponiamo che esista $z \in \{1, \dots, r\}$ tale che $v_x = t_{(z)}$. Dobbiamo allora distinguere alcuni casi:

  1. Supponiamo $z \neq w$; allora:
     - gli elementi del tipo $\eta_{(t_{(z)},y)}$ con $y \ge 2$ appartengono ad N per costruzione. In questo caso quindi
     $$\eta_{(t_{(z)},y)}^{p^{n_x}} \in N \subset N_i.$$
     - Gli elementi del tipo $\eta_{(t_{(z)},1)}$ sono proprio quelli della forma $\eta_{(z)}$. Allora come nella dimostrazione precedente:
       ∗ Se $z \neq r$ si ha:
       $$\eta_{(v_x,1)} = \eta_{(z)} = \begin{cases} \eta_{(1)} \in N_0 = N_{i_1-1} & \text{se } z = 1 \\ \eta_{(1)}^{p^{i_z-1}} \varepsilon_z \in N_{i_z-1} & \text{se } z \ge 2 \end{cases}$$
       da cui quindi $\eta_{v_x}^{p^{n_x}} \in N_{n_x+i_z-1}$.

∗ Se invece $z = r$ allora:

$$\eta_{(v_x,1)} = \eta_{(r)} = \begin{cases} \eta_{(1)} \in N_0 = N_{i_1-1} & \text{se } r = 1 \\ \eta_{(1)}^{-p^{i_r-1}} \varepsilon_r \in N_{i_r-1} & \text{se } r \geq 2 \end{cases}$$

da cui si ha comunque che $\eta_{(v_x,1)}^{p^{n_x}} \in N_{n_x+i_r-1}$.

Con lo stesso ragionamento precedente si ha che $i_z + n_x \geq i+1$ e quindi $N_{n_x+i_z-1} \subset N_i$.

2. Supponiamo invece $z = w$; allora:
   - gli elementi del tipo $\eta_{(t_{(w)},y)}$ con $1 \leq y < f$ appartengono ad N per costruzione. In questo caso quindi
   $$\eta_{(t_{(w)},y)}^{p^{n_x}} \in N \subset N_i.$$
   - Dimostriamo che l'elemento $t_{(t_{(w)},f)} \in N_i$. Infatti notiamo che per ipotesi $1 \leq w \leq r-1$; allora:
   $$\eta_{(t_{(w)},f)} = \eta_{(w)} = \begin{cases} \eta_{(1)} \in N_0 = N_{i_1-1} & \text{se } w = 1 \\ \eta_{(1)}^{p^{i_w-1}} \varepsilon_w \in N_{i_w-1} & \text{se } w \geq 2 \end{cases}$$
   D'altra parte anche per $z = w$ si ha che $i_w + n_x \geq i+1$ e quindi $N_{n_w+i_z-1} \subset N_i$.

Di conseguenza $U^{t^i+1} \subset N$, da cui segue la tesi in questo caso.

Caso b

Supponiamo che $t_{(r)} = \lambda_l = pe'$ e $t^{i_r-i} < \lambda_{l-i}$ $\forall i = 1, \ldots, l$. Notiamo che in questo caso vale la condizione $D(I)$ del teorema di Miki (in quanto se $t_{(r)} = t^{i_r} = pe'$ vuol dire che $pe' \in J$, quindi dalla definizione di J si vede che necessariamente $t^{i_r-1} < e'$). Assumiamo quindi, in accordo con il teorema di Miki, che $m \leq i_r - 1 + s$.
$\forall z \in \{1, \ldots, r\}$, poniamo

$$\eta_{(z)} = \eta_{(t_{(z)},1)} \quad \text{e} \quad \varepsilon_z = \eta_{(1)}^{-p^{i_z-1}} \eta_{(z)}.$$

Consideriamo allora il sottogruppo N di K^* definito nel modo seguente:

$$N =< K^{*p^m}, \pi, \eta_{(x,y)} \text{ con } x \in F - F_1, \varepsilon_z \text{ se } z = 2, \ldots, r > .$$

Dimostriamo che l'estensione L/K associata al sottogruppo N utilizzando la corrispondenza della class field è ciclica, totalmente ramificata di grado p^m e che ha come salti dell'estensione proprio $\{t^1, \ldots, t^m\}$. Infatti:

- Poiché $\pi \in N$ l'estensione associata ad N è totalmente ramificata.
- Vogliamo dimostrare che K^*/N è ciclico di ordine p^m e che precisamente è generato da $\eta_{(1)}N$. Notiamo che, per il lemma di decomposizione, possiamo scrivere ζ_s nella forma:

$$\zeta_s = \xi_l \xi_{l-1}^p \dots \xi_0^{p^l}.$$

Inoltre, dalla definizione di N, $\xi_i \in N \ \forall i = 0, \dots, l-1$; di conseguenza

$$\zeta_s \equiv \xi_l \quad (N).$$

D'altra parte, dalla condizione per cui $\lambda_l = t_{(r)}$ si ha che $\xi_l = \eta_{(1)}^{p^{i_r-1}} \varepsilon_r$ e $\varepsilon_r \in N$, da cui

$$\zeta_s \in \eta_{(1)}^{p^{i_r-1}} N.$$

Tuttavia dal teorema di Miki poiché vale la condizione $D(I)$ assumiamo che $m \leq i_r - 1 + s$. In questo caso la relazione di dipendenza lineare tra i generatori di U_K^1 diventa

$$1 = \eta_{(1)}^{p^{i_r+s-1}} \Big(\prod_{i=0}^{l-1} \xi_i^{p^{l-i}}\Big)^{p^s}.$$

Ciò mostra quindi che per costruzione $\eta_{(1)} \notin N$ e, poiché $m \leq i_r - 1 + s$ e $\eta_{(1)}^{p^m} \in N$ allora l'ordine di $\eta_{(1)}N$ in K^*/N è p^m. Per mostrare che non ci sono classi oltre quelle generate da $\eta_{(1)}N$ facciamo vedere che ognuno dei generatori di U^1 diverso da $\eta_{(1)}$ è in una di tali classi.
Consideriamo $\eta_{(x,y)}$ e distinguiamo due casi:

  - se $(x, y) \in F - F_1$ allora $\eta_{(x,y)} \in N$ per costruzione;
  - supponiamo $(x, y) \in F_1$; allora $y = 1$ ed esiste $z \in \{2, \dots r\}$ tale che $\eta_{(x,y)} = \eta_{(z)}$. In questo caso si ha

$$\eta_{(x,y)} = \eta_{(z)} = \eta_{(1)}^{p^{i_z-1}} \varepsilon_z \in \eta_{(1)}^{p^{i_z-1}} N.$$

Di conseguenza K^*/N è un gruppo ciclico di grado p^m e l'estensione associata è ciclica di grado p^m per le proprietà della teoria della class field.

Dimostriamo ora che i salti in alto della ramificazione dell'estensione L/K sono esattamente $t^1, \dots, t^m$.

$\forall 1 \leq i \leq m$ indichiamo con $N_i = NK^{*p^i}$. Come nei casi precedenti basta quindi dimostrare che $\forall i \in \{1, \dots, m\}$ si ha $U^{t^i} \not\subset N_i$ e $U^{t^i+1} \subset N_i$. Osserviamo che il gruppo N appena considerato ha la stessa forma del gruppo

usato nella costruzione fatta nel caso in cui $t_{(r)} \neq pe'$ oppure $\lambda_l \neq pe'$, e che la dimostrazione delle proprietà $U^{t^i} \not\subset N_i$ e $U^{t^i+1} \subset N_i$ dipende soltanto dalla forma del gruppo e non dalla classe di ζ_s modulo N. Di conseguenza applicando esattamente la stessa dimostrazione fatta nell'altro caso si ha che N soddisfa le proprietà richieste.

Caso c

Supponiamo infine che $t_{(r)} = \lambda_l = pe'$ e che esista $1 \leq J \leq l$ tale che $t^{i_r-J} > \lambda_{l-J}$. Poniamo allora:

- $\eta_{(z)} = \eta_{(t_{(z)},1)} \ \forall z \in \{1, \dots, r\}$;
- $\eta_0 = \eta_{(1)}^{p^{i_r-1-J}} \eta_{(\lambda_{l-J},f)}$;
- $\varepsilon_z = \eta_{(1)}^{-p^{i_z-1}} \eta_{(z)} \ \forall z \in \{2, \dots, r\}$.

Consideriamo allora il sottogruppo N di K^* definito nel modo seguente:

$$N =< K^{*p^m},\ \pi,\ \eta_{(x,y)} \text{ con } x \in F - F_1 - \{(\lambda_{l-J}, f)\},\ \eta_0,\ \varepsilon_z \text{ se } z = 2, \dots, r > .$$

Dimostriamo che l'estensione L/K associata al sottogruppo N utilizzando la corrispondenza della class field è ciclica, totalmente ramificata di grado p^m e che ha come salti dell'estensione proprio $\{t^1, \dots, t^m\}$.

- Osserviamo innanzitutto che l'estensione L/K è totalmente ramificata in quanto $\pi \in N$.
- Dimostriamo che $\zeta_s \in N$. Dal lemma di decomposizione abbiamo che ζ_s può essere scritto come

  $$\zeta_s = \xi_l \xi_{l-1}^p \dots \xi_0^{p^l}.$$

  Notiamo inoltre che dalla definizione del sistema dei generatori di U^1 scelto abbiamo che $\xi_i = \eta_{(x,f)}$ se $x = \lambda_i \in I$ e $\eta_{(pe',1)} = \xi_l$ se $\lambda_l = pe'$. Di conseguenza dalla costruzione del sottogruppo N abbiamo che $\xi_i \in N$ se $i \neq l$ e $i \neq l - J$. Scriviamo allora ζ_s come:

  $$\zeta_s = \xi_l \xi_{l-J}^{p^J} \prod_{i \neq l,\ l-J} \xi_i^{p^{l-i}}.$$

  Mostriamo allora che $\xi_l \xi_{l-J}^{p^{l-J}} \in N$; per fare ciò calcoliamo $\varepsilon_r \varepsilon_{i_r-J}^{p^J}$:

  $$\begin{aligned} \varepsilon_r \varepsilon_0^{p^J} &= \eta_{(1)}^{-p^{i_r-1}} \eta_{(r)} \big(\eta_{(1)}^{p^{i_r-1-J}} \eta_{(\lambda_{l-J},f)}\big)^{p^J} \\ &= \eta_{(1)}^{-p^{i_r-1}} \eta_{(r)} \eta_{(1)}^{p^{i_r-1}} \eta_{(\lambda_{l-J},f)}^{p^J} = \xi_l \xi_{l-J}^{p^J}. \end{aligned}$$

  Si vede quindi che $\zeta_s \in N$ perché prodotto di elementi di N.

- Dimostriamo che K^*/N è ciclico di ordine p^m e precisamente generato da $\eta_{(1)}N$.
  Infatti le classi $N, \eta_{(1)}N, \eta_{(1)}^2N, \dots, \eta_{(1)}^{p^m-1}N$ sono tutte distinte in quanto nessuna delle potenze $\eta_{(1)}^i$ con $i \leq p^m - 1$ appartiene al sottogruppo N.
  Per mostrare che questi sono gli unici elementi di K^*/N mostriamo che tutti gli altri generatori di U^1 diversi da $\eta_{(1)}$ appartengono ad una delle classi di equivalenza descritte sopra. Distinguiamo vari casi:

  - se $(x,y) \in F - F_1 \cup \{(\lambda_{l-J}, f)\}$, allora per costruzione abbiamo che $\eta_{(x,y)} \in N$.
  - Supponiamo $(x,y) \in F_1$; allora $y = 1$ ed esiste $z \in \{2, \dots r\}$ tale che $\eta_{(x,y)} = \eta_{(z)}$. In questo caso allora
    $$\eta_{(x,y)} = \eta_{(z)} = \eta_{(1)}^{p^{i_z-1}} \varepsilon_z \in \eta_{(1)}^{p^{i_z-1}} N.$$
  - Supponiamo infine che $(x,y) = (\lambda_{l-J}, f)$; allora
    $$\eta_{(\lambda_{l-J},f)} = \eta_{(1)}^{-p^{i_r-1-J}} \eta_0 \in \eta_{(1)}^{-p^{i_r-1-J}} N.$$

  Di conseguenza K^*/N è ciclico di ordine p^m e per le proprietà date dalla class field l'estensione L/K associata ad N è ciclica di grado p^m come voluto.

Dimostriamo ora che i salti della ramificazione dell'estensione L/K sono esattamente $t^1, \dots, t^m$.

$\forall 1 \leq i \leq m$ indichiamo con $N_i = NK^{*p^i}$. Come nei casi precedenti basta dimostrare che $\forall i \in \{1, \dots, m\}$ si ha $U^{t^i} \not\subset N_i$ e $U^{t^i+1} \subset N_i$.

Anche in questo caso la dimostrazione della proprietà $U^{t^i} \not\subset N_i$ è identica a quella nel caso in cui $\overline{K} \neq \mathbb{F}_p$ e $\zeta_p \notin K$ (basta prendere u il maggior elemento di $\{1, \dots, r\}$ tale che $t_{(u)} \leq t^i$ e si dimostra allo stesso modo che $\eta_{(u)}^{p^{i-i_u}}$ è un elemento di U^{t^i} che non appartiene ad N_i).
Dimostriamo allora che $U^{t^i+1} \subset N_i$.
$\forall x \geq t^i + 1$ sia n_x il più piccolo intero tale che $x = f^{n_x}(v_x)$ con $v_x \in I'$. Notiamo allora che in questo caso U^{t^i+1} è generato dagli elementi della forma $\{\eta_{(v_x,y)}^{p^{n_x}}\}$ con $x \geq t^i + 1$ e y che varia nell'insieme $\{1 \dots f\}$ se $v_x \neq pe'$ oppure è uguale ad 1 se $v_x = pe'$. Vogliamo mostrare che gli elementi di questa forma appartengono a N_i.
Distinguiamo vari casi:

- supponiamo $v_x \neq t_{(z)}$ $\forall z \in \{1, \dots, r\}$ e $v_x \neq \lambda_{l-J}$, allora $\eta_{(v_x,y)} \in N$ $\forall 1 \leq y \leq f$ e quindi $\eta_{(v_x,y)}^{p_x^n} \in N \subset N_i$;

- supponiamo $v_x = \lambda_{l-J}$. Distinguiamo due ulteriori casi:
  - se $y \in \{1 \ \dots f-1\}$ allora $\eta_{(\lambda_{l-J},y)} \in N$, da cui $\eta_{(\lambda_{l-J},y)}^{p_x^n} \in N \subset N_i$;
  - se $y = f$, allora

    $$\eta_{(\lambda_{l-J},f)} = \eta_{(1)}^{-p^{i_r-1-J}} \eta_0 \in N_{i_r-1-J},$$

    da cui

    $$\eta_{(\lambda_{l-J},f)}^{p^{n_x}} \in N_{i_r-1-J-n_x}.$$

    Dimostriamo che $N_{i_r-1-J-n_x} \subset N_i$. Distinguiamo dunque due casi:
    - se $i_r - J + n_x \geq m+1$, allora banalmente $i_r - J + n_x \geq i+1$ e quindi si ha l'inclusione;
    - supponiamo $i_r - J + n_x \leq m$; dalle ipotesi su x sappiamo che:

      $$t^i + 1 \leq x = f^{n_x}(v_x) = f^{n_x}(\lambda_{l-J}) < f^{n_x}(t^{i_r-J}) \leq t^{i_r-J+n_x}.$$

      Si ha quindi $i+1 \leq i_r - J + n_x$, da cui $N_{i_r-1-J-n_x} \subset N_i$.

- Supponiamo che esista $z \in \{1, \dots, r\}$ tale che $v_x = t_{(z)}$. Allora:
  - se $y \in \{2, \dots, f\}$ allora $\eta_{(t_{(z)},y)} \in N$ per costruzione, e quindi anche $\eta_{(t_{(z)},y)}^{p^{n_x}} \in N \subset N_i$.
  - se $y = 1$ allora si ha:

    $$\eta_{(v_x,1)} = \eta_{(z)} = \begin{cases} \eta_{(1)} \in N_0 = N_{i_1-1} & \text{se } z = 1 \\ \eta_{(1)}^{p^{i_z-1}} \varepsilon_z \in N_{i_z-1} & \text{se } z \geq 2 \end{cases}$$

    da cui quindi $\eta_{v_x}^{p^{n_x}} \in N_{n_x+i_z-1}$. Con gli stessi conti delle sezioni precedenti si ha che $i_z + n_x \geq i+1$ e quindi $N_{n_x+i_z-1} \subset N_i$.

Ciò mostra quindi che $U^{t^i+1} \subset N_i$, da cui la tesi.

Capitolo 8

Esempi

In questo capitolo vogliamo dare alcune applicazioni del teorema di Miki. In particolare daremo un metodo per il calcolo dell'invariante definito da $I(K) = \{s; \lambda_0, \lambda_1, \ldots, \lambda_l\}$ in alcuni casi particolari del campo K e, a partire da questo, un esempio di applicazione del teorema.

8.1 Un caso semplice

Analizziamo per prima cosa il caso in cui $K = \mathbb{Q}_p(\zeta_s)$, dove con ζ_s indichiamo come al solito una radice p^s-esima dell'unità. In questo caso, come abbiamo visto nel secondo capitolo, $v_K(\zeta_s - 1) = 1$, quindi $v_K(\zeta_s - 1) \not\equiv 0 \ (p)$. Sappiamo inoltre che $e = v_K(p) = p^{s-1}(p-1)$ ed $e' = e/(p-1) = p^{s-1}$.

Sia allora $\{t^1, t^2, \ldots, \}$ una insieme di interi tali che:

- $1 \leq t^1 \leq p^s$ e $(t^1, p) = 1$ se $t^1 \neq pe'$;
- se $t^i < p^{s-1}$, allora $pt^i \leq t^{i+1} \leq p^s$ e $(t^{i+1}, p) = 1$ se $t^{i+1} \neq pt^i, p^s$;
- se $t^i \geq p^{s-1}$ allora $t^{i+1} = t^i + p^{s-1}(p-1)$.

Valgono allora le due affermazioni seguenti:

- se $t^1 \neq 1$ allora esiste una $\mathbb{Z}_p$-estensione totalmente ramificata di $\mathbb{Q}_p(\zeta_s)$ con salti della ramificazione in alto $\{t^1, t^2, \ldots, \}$;
- se $t^1 = 1$ allora esiste un'estensione K_m/K ciclica totalmente ramificata di grado p^m con salti della ramificazione in alto $\{t^1, \ldots, t^m\}$ se e solo se $m \leq s$.

Esempio 8.1. *Consideriamo $K = \mathbb{Q}_p(\zeta_s)$ e $L = \mathbb{Q}_p(\zeta_{s+h})$ con $h \geq 1$; allora banalmente L/K è un'estensione ciclica totalemente ramificata di grado p^h. Vogliamo calcolarne i salti in alto della ramificazione.*
Ricordiamo che $e = v_K(p) = p^{s-1}(p-1)$ ed $e' = p^{s-1}$.

$$\begin{array}{c} L = \mathbb{Q}_p(\zeta_{s+h}) \\ \Big| \; p^h \\ K = \mathbb{Q}_p(\zeta_s) \\ \Big| \; p^{s-1}(p-1) \\ \mathbb{Q}_p \end{array}$$

Sia $H = Gal(L/K) \cong \mathbb{Z}/p^h\mathbb{Z}$ e $G = Gal(L/\mathbb{Q}_p) \cong \mathbb{Z}/p^{s+h}\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}$; allora dai calcoli fatti nel secondo capitolo sui salti delle estensioni ciclotomiche si vede che $H = G_{p^s-1}$. Utilizzando la proposizione 1.19 sappiamo che $\forall i \geq 1$ $H_i = H \cap G_i$.
Di conseguenza i salti in basso dell'estensione L/K sono uguali ai salti in basso dell'estensione $L/\mathbb{Q}_p$ che siano maggiori o uguali a $p^s - 1$. I salti in basso sono quindi $t_1 = p^s - 1$, $t_2 = p^{s+1} - 1, \ldots, t_h = p^{s+h-1} - 1$. Calcoliamo allora i rispettivi salti in alto utilizzando la funzione $\varphi = \varphi_{L/K}$. Precisamente mostriamo per induzione che

$$t^i = ip^s - (i-1)p^s - 1 \quad \forall 1 \leq i \leq h.$$

- *Passo base $i = 1$:*
  $t^1 = \varphi(t_1) = \dfrac{1}{p^h}(p^h t_1) = t_1 = p^s - 1$, *da cui $t^1 \geq e'$;*
- *Passo induttivo $i \to i+1$:*
  $t^{i+1} = \varphi(t_{i+1}) = t^i + p^{h-i}\dfrac{p^{s+i} - p^{s+i-1}}{p^h} = t^i + p^{s-1}(p-1) = (i+1)p^s - ip^{s-1} - 1.$

Si vede quindi che i salti in alto sono in accordo con le condizioni del teorema di Miki.

Nel caso generale la difficoltà nell'applicazione del teorema di Miki è la determinazione dell'invariante $I(K)$ (che non sempre è facile da calcolare). Nella prossima sezione daremo un metodo per calcolare $I(K)$ in alcuni casi particolari e vedremo un esempio di applicazione di tale metodo.

8.2 Una caratterizzazione dell'invariante $I(K)$

Vale il seguente risultato:

Proposizione 8.1. *Sia K_0 un campo completo rispetto ad una valutazione discreta con $char(K_0) = 0$ e $\overline{K_0} = p$ e supponiamo che $\zeta_1 \in K_0$.*

Fissiamo m un intero non negativo e $\forall i$ tale che $0 \leq i \leq m-1$ sia K_{i+1}/K_i un'estensione ciclica totalmente ramificata di grado p; chiamiamo con t^{i+1} il salto della ramificazione. Indichiamo inoltre con $e_{K_i} = v_{K_i}(p)$ e con $e'_{K_i} = e_{K_i}/(p-1)$.
Supponiamo che $t^m > t^{m-1} > \dots t^1$. Sia $\alpha \in U^1_{K_0}$ con $\lambda = v_{K_0}(\alpha - 1)$ tale che $1 \leq \lambda < pe'_{K_0}$ e $\lambda \not\equiv 0 \ (p)$.
Indichiamo con $s_{i+1} = \phi_{K_m/K_0}(t^{i+1})$ e supponiamo che $s_{i+1} \neq pe'_{K_0} - \lambda \ \forall i$ tale che $0 \leq i \leq m-1$.
Allora vale che $\lambda_i(\alpha; K_m) = \delta_{K_i/K_0}(\lambda)$ per $i = 0, 1, \dots m$, dove i $\lambda_i(\alpha; K_m)$ sono definiti come in 5.1 e

$$\delta_{K_i/K_0}(\lambda) = e'_{K_i}p - \psi_{K_i/K_0}(e'_{K_0}p - \lambda).$$

Una dimostrazione di tale proposizione (che non è di facile dimostrazione) può essere trovata su [Mik1].
Da tale proposizione discende facilmente il seguente corollario:

Corollario 8.2. *Sia p un primo e sia $\mathbb{Q}_p$ il campo dei numeri p-adici. Poniamo $K_0 = \mathbb{Q}(\zeta_s)$ per un numero naturale s. Sia K/K_0 un'estensione di Galois finita totalmente ramificata con $\zeta_{s+1} \notin K$ e sia l l'intero non negativo tale che $p^l \parallel [K : K_0]$. Denotiamo con $T(K/K_0)$ l'insieme dei salti della ramificazione con indici in alto e supponiamo che $(p^s - 1) \notin T(K/K_0)$.*
Allora l'invariante $I(K)$ è descritto esplicitamente usando $T(K/K_0)$.
Più precisamente se $I(K) = (s; \lambda_0, \dots \lambda_l)$ allora $\delta_{L_i/K_0}(1) = \lambda_i$ per $i = 0, 1 \dots l$, dove L_0 è la massima sottoestensione ramificata tame di K/K_0 e

$$K = L_l \supsetneq L_{l-1} \supsetneq \dots \supsetneq L_0 \supseteq K_0$$

è la successione dei distinti campi di ramificazione di K/K_0.

Osservazione 8.3. Nel corollario precedente il fatto che K/K_0 abbia $l+1$ salti della ramificazione (eventualmente l salti se $p^l = [K : K_0]$, cioé se l'estensione non ha parte tame) discende dalla proprietà per cui $\overline{K_0} = \mathbb{F}_p$ e dalla proposizione 4.12.

Utilizzando tale corollario possiamo fare il seguente esempio.

8.3 Esempio

Poniamo $K_0 = \mathbb{Q}_p(\zeta_2)$, dove con ζ_2 indichiamo come al solito una radice p^2-esime dell'unità.
Costruiamo due estensioni K_1 e K_2 di K_0 di grado p tali che i salti della ramificazione delle due estensioni siano rispettivamente 1 e $p+1$.

Notiamo che il teorema 4.6 del capitolo 4 ci dice che se K è un campo completo che contiene ζ_p e u_l è un elemento di U_K^1 tale che $v_K(u_l - 1) = l$ con $1 \leq l < pe/(p-1)$ e $(l,p) = 1$, allora $K(\sqrt[p]{u_l})/K$ è un'estensione totalmente ramificata di grado p con salto della ramificazione pari a $s = pe/(p-1) - l$.

Utilizzando tale risultato possiamo costruire facilmente K_1 e K_2. Infatti nel nostro caso:

$$e_{K_0} = e = p(p-1) \quad \text{e} \quad e'_{K_0} = e/(p-1) = p.$$

Di conseguenza, se u è un elemento di U_{K_0} tale che $v_K(u-1) = p^2 - 1$ allora l'estensione $K_1 = K_0(\sqrt[p]{u})/K_0$ è totalmente ramificata e il salto della ramificazione è proprio $t^1 = p^2 - (p^2 - 1) = 1$ come richiesto. Allo stesso modo, se v è un elemento di U_{K_0} tale che $v_K(v-1) = p^2 - p - 1$ allora l'estensione $K_2 = K_0(\sqrt[p]{u})/K_0$ è totalmente ramificata e il salto della ramificazione è proprio $t^2 = p^2 - (p^2 - p - 1) = p + 1$.

Consideriamo ora il composto delle due estensioni $k = K_1K_2$; allora il grado dell'estensione è pari a $[k : K_0] = p^2$, e siccome k ha due sottoestensioni distinte di grado p allora per la teoria di Galois

$$Gal(K_1K_2/K_0) \cong Gal(K_1/K_0) \times Gal(K_2/K_0) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

Dalla trattazione delle estensioni con gruppo di Galois $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ nel capitolo 4 sappiamo che l'estensione k/K_0 ha due salti della ramificazione che sono esattamente pari a $t^1 = 1$ e $t^2 = p + 1$.

Vogliamo adesso calcolare l'invariante del campo $I(k)$ utillizzando il corollario precedente. Per costruzione $K_0 = \mathbb{Q}_p(\zeta_2)$, dunque $\zeta_2 \notin k$.
Mostriamo che $\zeta_3 \notin k$. Supponiamo infatti per assurdo che $\zeta_3 \in k$; allora $K_0(\zeta_3)/K_0 = \mathbb{Q}_p(\zeta_3)/\mathbb{Q}_p(\zeta_2)$ è una sottoestensione di k/K_0 di Galois di grado p. Tuttavia per quanto visto nel capitolo 4 k/K_0 ha esattamente $p+1$ estensioni di grado p di cui una con salto della ramificazione uguale ad 1 e p con salto della ramificazione pari a $p+1$. Calcoliamo allora il salto dell'estensione $\mathbb{Q}_p(\zeta_3)/\mathbb{Q}_p(\zeta_2)$ e mostriamo che è diverso da 1 e da $p+1$ (dunque $\mathbb{Q}_p(\zeta_3) \neq K_1, K_2$).

Per fare ciò usiamo i calcoli fatti nell'esempio 8.1; abbiamo infatti dimostrato che nel caso di un'estensione della forma $\mathbb{Q}_p(\zeta_{s+h})/\mathbb{Q}_p(\zeta_s)$ allora i

salti in alto della ramificazione sono $t^1 = p^s - 1, \dots t^h = p^{s+h-1} - 1$. Nel nostro caso allora abbiamo che $s = 2$ e $h = 1$, quindi l'estensione ha un unico salto della ramificazione che è pari a $p^2 - 1$. Di conseguenza $\mathbb{Q}_p(\zeta_3) \neq K_1, K_2$, da cui $\zeta_3 \notin k$.
Abbiamo quindi dimostrato che $I(k) = (2; \lambda_0, \lambda_1, \lambda_2)$.
Per calcolare i λ_i usiamo il corollario precendente. Se L_0 è la massima sottoestensione totalmente ramificata tame di K_0 in k, e $k = L_2 \supsetneq L_1 \supsetneq L_0 \subseteq K_0$ è la sequenza dei campi di ramificazione distinti di k/K_0, allora si ha che $\lambda_i = \delta_{L_i/K_0}(1)$.

$$
\begin{array}{c}
K_1K_2 \\
\Big| \; p \\
K_1 \\
\Big| \; p \\
\mathbb{Q}_p(\zeta_2) \\
\Big| \; p(p-1) \\
\mathbb{Q}_p
\end{array}
$$

1. L'estensione k/K_0 è di tipo wild, quindi la massima sottoestensione tame di k/K_0 è $L_0 = K_0$.
   Allora $\lambda_0 = \delta_{K_0/K_0}(1) = 1$.

2. $\lambda_1 = \delta_{K_1/K_0}(1)$; ricordiamo che da definizione si ha che

   $$\delta_{K_1/K_0}(1) = e'_{K_1}p - \psi(e'_{K_0}p - 1).$$

   Notiamo inoltre che:

   - $e_{K_0} = p(p-1)$, dunque $e'_{K_0} = p$ e $e'_{K_1} = p^2$;
   - $\psi_{K_1/K_0}(e'_{K_0}p - 1) = \psi_{K_1/K_0}(p^2 - 1) = p\left(\frac{1}{p} + p^2 - 2\right)$
     $= (1 + p^3 - 2p) = p^3 - 2p + 1$;

   quindi $\delta_{K_1/K_0}(1) = p^3 - 1 - p^3 + 2p = 2p - 1$.

3. $\lambda_2 = \delta_{K_1K_2/K_0}(1)$; in questo caso si ha che:

   - $e'_{K_1K_2} = p^3$;
   - $T(K_1K_2/K_0) = \{1, p+1\}$;

- $\psi_{K_1K_2/K_0}(p^2-1) = p^2\left(\frac{1}{p^2}+\frac{p}{p}+p^2-1-(p+1)\right)$
  $= (1+p^2+p^4-p^3-2p^2) = p^4-p^3-p^2+1;$

quindi $\delta_{K_1K_2/K_0}(1) = p^4-p^4+p^3+p^2-1 = p^3+p^2-1$.

Dunque $I(k) = (2;1,2p-1,p^3+p^2-1)$.

Vogliamo ora vedere qualche applicazione del teorema di Miki.

8.4 Applicazioni del teorema di Miki

8.4.1 Esempio 1

Sia k il campo costruito nella sezione precedente.
Supponiamo $t^1 = \lambda_1,\ t^2 = p\lambda_1,\ t^3 = p^2\lambda_1$. Indichiamo come al solito con n il minimo intero tale che $t^n \geq e'$. Osserviamo che l'estensione $k/\mathbb{Q}_p$ è totalmente ramificata, quindi $\overline{k} = \mathbb{F}_p$. Mostriamo che vale la condizione $C(j)$ del teorema di Miki per $j = 2$.
Ricordiamo che la condizione $C(j)$ dice che:

$C(j)$ Esiste un sottoinsieme T di $\{0,1\dots l\}$ tale che:

- $t^{j-i} = \lambda_{l-i} \quad \forall i \in T;$
- $t^{j-i} < \lambda_{l-i} \quad \forall i \in \{0,1\dots l\} - T,$

e la cardinalità dell'insieme T è 1 se $p \neq 2$ e dispari se $p = 2$.

Osserviamo che nel nostro caso $e'_k = p^3$; di conseguenza, essendo $\lambda_1 = 2p-1$, si ha:

- $t^1 = 2p-1;$
- $t^2 = p(2p-1) = 2p^2-p;$
- $t^3 = 2p^3-p^2.$

Allora, $t^2 = 2p^2-p < e'$ e $p^3 \leq 2p^3-p^2 = t_3$, da cui in questo caso $n = 3$.

Prendiamo dunque $j = 2$ e $T = \{1\}$. Allora:

- $t^{j-i} = t^1 = \lambda_{2-i} = \lambda_1$;
- $t^{j-i} < \lambda_{2-i}\ \forall i = 0, 2$. Infatti:
  - Se $i = 0$, $t^2 = 2p^2 - p < \lambda_2 = p^3 + p^2 - 1 \iff$
    $p^3 - p^2 + p - 1 > 0 \iff$
    $(p^2 + 1)(p - 1) > 0 \iff p > 1$, dunque la condizione è verificata.
  - Se $i = 2$, $t^0 = 0 < \lambda_0 = 1$.

Di conseguenza la condizione $C(j)$ vale per $j = 2$.
Notiamo che $\{t^1, t^2, t^3\}$ soddisfano le condizioni necessarie del teorema di Miki. Infatti:

- $t^1 = 2p - 1$ quindi $1 < t^1 < p^4$ con $(t^1, p) = 1$;
- $t^2 = 2p^2 - p$ quindi $pt^1 = t^2$;
- $t^3 = 2p^3 - p^2$ quindi $t^3 = pt^2$.

Osserviamo che $j \geq n - s + 1$, infatti $n - s + 1 = 3 - 2 + 1 = 2$ e abbiamo dimostrato che $j = 2$.
Il teorema di Miki in questo caso ci dice che, poiché vale la condizione $C(j)$ per $j = 2$ allora esiste un'estensione ciclica totalmente ramificata di grado p^m con salti della ramificazione dati precedentemente se e solo se $m \leq j + s - 1$, che nel nostro caso è uguale a 3.

Vogliamo utilizzare la costruzione del capitolo 7 per esibire il sottogruppo normico associato ad un'estensione L/k ciclica totalmente ramificata e di grado p^3 con salti in alto della ramificazione $\{2p - 1,\ 2p^2 - p,\ 2p^3 - p^2\}$.
Ricordiamo che in questo caso $e'_k = p^3$ ed $e_k = p^3(p - 1)$. Siano ξ_0, ξ_1 e ξ_2 gli elementi dati dal lemma di decomposizione tali che:

$$\zeta_2 = \xi_2 \xi_1^p \xi_0^{p^2}.$$

Definiamo allora

$$I = \{1 \leq x < p^4 \mid (x, p) = 1\} \quad \text{e} \quad I' = I \cup \{p^4\}.$$

Indichiamo inoltre con $J_1 = \{t_{(1)}\} = \{2p - 1\}$ (notiamo che $t^2, t^3 \notin J_1$ in quanto $t^2 = pt^1$ e $t^3 = pt^2$). Sia π un uniformizzante di k. Notiamo che $\overline{k} = \mathbb{F}_p$, quindi possiamo prendere come sistema di generatori di U_k^1 definito nel modo seguente:

- $\eta_x = 1 + \pi^x$ se $x \in I' - \{\lambda_0, \lambda_1, \lambda_2\}$;
- $\eta_x = \xi_i$ se esiste $i = 0, 1, 2$ tale che $x = \lambda_i$.

Allora, se consideriamo il sottogruppo N di k^* definito da

$$N =< k^{*p^3},\ \pi,\ \eta_x\ (x \in I' - J_1) >,$$

l'estensione associata ad N tramite la class field soddisfa le proprietà richieste.

8.4.2 Esempio 2

Supponiamo invece $t^1 = 1,\ t^2 = p,\ t^3 = 1 + p^3,\ t^4 = 1 + p^4$ e $t^5 = 1 + p^3 + 2p^4$. Mostriamo che in questo caso vale $C(j)$ per $j = 3$. Prendiamo infatti $T = \{2\}$; allora:

- Se $i = 2$, $t^{j-i} = t^1 = 1 = \lambda_{l-2} = \lambda_0$;
- Se $i = 0$, $t^{j-i} = t^3 = 1 + p^3 < \lambda_{l-0} = \lambda_{2-0} = p^3 + p^2 - 1$;
- Se $i = 1$, $t^{j-i} = t^2 = p < \lambda_1 = 2p - 1$.

Vale quindi $C(j)$ per $j = 3$. Notiamo inoltre che anche in questo caso $e'_k = p^3$ e $e_k = p^3(p-1)$; allora $p^3 < 1 + p^3 = t^3$, da cui $n = 3$.
Mostriamo che $\{t^1, \ldots, t^5\}$ soddisfano le condizioni necessarie del teorema di Miki:

- $t^1 = 1$ quindi $1 \leq t^1 < p^4$ con $(t^1, p) = 1$;
- $t^2 = p$ quindi $t^2 = pt^1$;
- $t^3 = 1 + p^3$ quindi $p^2 < t^3 < p^4$ e $(t^3, p) = 1$; inoltre $t^3 \geq p^3$;
- $t^4 = 1 + p^4 = 1 + p^3 + p^3(p-1) = t^3 + e$;
- $t^5 = 1 + 2p^4 + p^3 = 1 + p^3 + p^3(p-1) = t^4 + e$.

Allora, applicando il teorema di Miki, poiché anche in questo caso $\overline{k} = \mathbb{F}_p$, si ha che esiste un'estensione k_m di k ciclica totalmente ramificata di grado p^m con salti della ramificazione $\{t^1, \ldots t^m\} \iff m \leq j + s - 1 = 3 + 2 - 1 = 4$. In particolare quindi non esistono estensioni di k cicliche totalmente ramificate di grado p^5 con salti della ramificazione in alto $\{1,\ p,\ 1{+}p^3,\ 1{+}p^4,\ 1{+}p^3{+}2p^4\}$.

Anche qui usiamo la la costruzione del capitolo 7 per esibire il sottogruppo normico associato ad un'estensione L/k ciclica totalmente ramificata e di

grado p^4 con salti in alto della ramificazione $\{1,\ p,\ 1+p^3,\ 1+p^4\}$.
Ricordiamo che in questo caso $e'_k = p^3$ ed $e_k = p^3(p-1)$. Siano ξ_0, ξ_1 e ξ_2 gli elementi dati dal lemma di decomposizione tali che:

$$\zeta_2 = \xi_2 \xi_1^p \xi_0^{p^2}.$$

Definiamo allora

$$I = \{1 \le x < p^4 \mid (x,p) = 1\} \quad \text{e} \quad I' = I \cup \{p^4\}.$$

Indichiamo inoltre con $J_1 = \{t_{(1)}, t_{(2)}\} = \{1, 1+p^3\}$ (notiamo che $t^2 \notin J_1$ in quanto $t^2 = pt^1$ e $t^4 \notin J_1$ perché $t^4 = t^3 + e$). Sia π un uniformizzante di k. Consideriamo il sistema di generatori $\{\eta_x\}_{x \in J'}$ di U_k^1 definito nell'esempio precedente. Notiamo che $t_{(2)} = t^3$, quindi $i_2 = 3$; definiamo quindi

$$\varepsilon_2 = \eta_1^{-p^2} \eta_{1+p^3} = \xi_0^{-p^2} \eta_{1+p^3}.$$

Allora, se consideriamo il sottogruppo N di k^* definito da

$$N = < k^{*p^3},\ \pi,\ \eta_x\ (x \in I' - J_1), \varepsilon_2 >,$$

l'estensione associata ad N tramite la class field soddisfa le proprietà richieste.

Osservazione 8.4. Notiamo che $\zeta_2 = \xi_0^{p^2} \xi_1^p \xi_2 \equiv \xi_0^{p^2}\ (N)$, quindi

$$\zeta_1 = \zeta_2^p = \xi_2^{p^3} \xi_1^{p^2} \xi_0^p \equiv \xi_0^{p^3}\ (N).$$

Vale quindi che $\zeta_1 \notin N$. Per il teorema 6.17 si ha che l'estensione L/K associata ad N non può essere immersa in un'estensione M/k ciclica e totale di grado p^5. Ciò è in accordo con il teorema di Miki.

Bibliografia

[AlB] J.L.Alperin, R.B.Bell,
Groups and representations,
GTM, Springel Verlag (1995).

[Arf] C.Arf,
Untersuchungen über reinverzweigte Erweiterungen diskret bewerteter perfekter Körper,
J.Reine Angew. Math. 181 (1939), pp. 1-44.

[ArT] E.Artin, J.Tate,
Class field theory,
New York-Amsterdam (1968).

[Bos] S.Bosch,
Algebra,
Springer Verlag, 2003.

[Bou] N.Bourbaki,
Commutative Algebra,
Springer-Verlag, 1981.

[CFr] J.W.S. Cassels, A. Frölich,
Algebraic Number Theory,
Academic Press, 1967.

[DCD] I.Del Corso, R.Dvornicich,
The compositum of wild extensions of local fields of prime degree,
Monatsh. Math. 150 (2007), pp. 271-288.

[FeV] I.B.Fesenko, S.V. Vostokov,
Local fields and their extensions,
2nd Edition, American Mathematical Society, 2002.

[Fes] I.B.Fesenko,
Hasse-Arf Property and Abelian Extensions,
Math. Nachr. 174 (1994), pp. 81-87.

[Fon] J.M. Fontaine,
Groupes de ramification et représentations d'Artin,
Ann. Scient. Ec. Norm. Sup. 4 (1971), pp. 337-392.

[Hel] C.Helou,
On the ramification breaks,
Communications in Algebra, 19 (1991), pp.2267-2279.

[La1] S.Lang,
Algebraic Number Theory,
3nd Edition, Springer Verlag, 2002.

[La2] S.Lang,
Algebra,
3rd edition, Springer Verlag, 2002.

[Mar] M.A.Marshall,
The Maximal p-extension of a local field,
Can. J. Math., Vol XXIII, No. 3 (1971), pp.398-402.

[Mau1] E.Maus,
On the jumps in the series of ramification groups, Colloque de Theorie des Nombres (Bordeaux 1969),
Bull.Soc.math.France, Mémoire 25 (1971), pp.127-133.

[Mau2] E.Maus,
Relationen in Verzweinsgruppen,
J.reine angew. Math. 258 (1973), pp. 23-50.

[Mik1] H.Miki,
On the ramification numbers of cyclic p-extensions over a local fields,
J.Reine Angew. Math. 328 (1981), pp. 99-115.

[Mik2] H.Miki,
A note on Maus' theorem on ramification groups,
Tohoku Math. J. 29 (1977), pp.61-68.

[Neu] J.Neukirch,
Algebraic Number Theory,
Springer Verlag, 1986.

[Ngu] T.Nguyen-quang-do,
Filtration de K^*/K^{*p} et ramification sauvage,
Acta Arith. 30 (1976), pp. 323-340.

[ObP] A.Obus, R.Pries,
Wild tame-by-cyclic extentions,
Journal of Pure and Applied Algebra 214 (2010), pp. 565-573.

[Ser] J.P.Serre,
Local fields,
Springer Verlag, 1979.

[Sue1] Y.Sueyoshi,
Ramification numbers of cyclic p-extentions over p-adic number fields,
Mem. Fac. Sci., Kyushu University Sez. A, 38, No. 2 (1984), pp. 163-168.

[Sue2] Y.Sueyoshi,
On ramification of p-extensions of p-adic number fields,
Mem. Fac. Sci., Kyushu University Sez. A, 32, No. 2 (1977), pp. 199-204.

[Viv] F.Viviani,
Ramification Groups and Artin Conductors of Radical Extensions of $\mathbb{Q}$,
J. Thor. Nombres Bordeaux 16 (2004), pp. 779-816.

[Wym] B.F.Wyman,
Wildly Ramified Gamma Extensions,
Amer. J. oh Math. 91 (1969), pp. 135-152.